8046-1041
PATENT

IN THE U.S. PATENT AND TRADEMARK OFFICE

Applicant:	Masayuki NAKAE et al.	Confirmation No. Unknown
Appl. No.:	10/643,864	Group: Unknown
Filed:	August 20, 2003	Examiner: Unassigned
For:	ATTACK DEFENDING SYSTEM AND ATTACK DEFENDING METHOD	

L E T T E R

Assistant Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Date: December 1, 2003

Sir:

Under the provisions of 35 U.S.C. § 119 and 37 C.F.R. § 1.55(a), the applicant(s) hereby claim(s) the right of priority based on the following application(s):

Country	Application No.	Filed
Japan	2002-238989	August 20, 2002
Japan	2003-074781	March 19, 2003
Japan	2003-295020	August 19, 2003

Certified copies of the above-noted applications are attached hereto.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 25-0120 for any additional fee required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Respectfully submitted,

YOUNG & THOMPSON

By Benoît Castel

Benoît Castel, Reg. No. 35,041
745 South 23rd Street, Suite 200
Arlington, Virginia 22202
(703) 521-2297

Attachments

87 US

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年　８月２０日

出願番号
Application Number: 特願２００２－２３８９８９

[ST. 10/C]: ［ＪＰ２００２－２３８９８９］

出願人
Applicant(s): 日本電気株式会社

２００３年　８月２０日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０６８００６

【書類名】　特許願
【整理番号】　35001159
【提出日】　平成14年 8月20日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 12/22
　　G06F 13/00
【発明者】
　【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
　【氏名】　中江　政行
【発明者】
　【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
　【氏名】　山形　昌也
【特許出願人】
　【識別番号】　000004237
　【氏名又は名称】　日本電気株式会社
【代理人】
　【識別番号】　100097157
　【弁理士】
　【氏名又は名称】　桂木　雄二
【手数料の表示】
　【予納台帳番号】　024431
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9303562
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　攻撃防御システムおよび攻撃防御方法

【特許請求の範囲】

【請求項１】　内部ネットワークと外部ネットワークとの境界に設置され、おとり装置およびファイアウォール装置を含む攻撃防御システムにおいて、

前記おとり装置は、

前記ファイアウォール装置から転送された入力ＩＰパケットに対するサービスプロセスを実行することで攻撃の有無を検知する攻撃検知手段を有し、

前記ファイアウォール装置は、

入力ＩＰパケットのヘッダ情報およびフィルタリング条件に基づいて、当該入力ＩＰパケットを受理するか否かを判定するパケットフィルタリング手段と、

受理された入力ＩＰパケットのヘッダ情報および振り分け条件に基づいて、当該入力ＩＰパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、

前記おとり装置へ転送した入力ＩＰパケットに関して前記攻撃検知手段が攻撃を検知したか否かに基づいて、当該入力ＩＰパケットに対応するフィルタリング条件を管理するフィルタリング条件管理手段と、

を有することを特徴とする攻撃防御システム。

【請求項２】　入力ＩＰパケットの前記ヘッダ情報は当該入力ＩＰパケットの送信元ＩＰアドレスおよび宛先ＩＰアドレスの少なくとも一方であり、

前記転送先選択手段は前記入力ＩＰパケットのヘッダ情報が前記振り分け条件を満たすか否かに依存して当該入力ＩＰパケットの転送先を決定する、

ことを特徴とする請求項１記載の攻撃防御システム。

【請求項３】　前記転送先選択手段は、

前記内部ネットワークで使用されていないＩＰアドレスからなる誘導リストを前記振り分け条件として保持する格納手段を有し、

前記入力ＩＰパケットの宛先ＩＰアドレスと前記誘導リスト内の未使用ＩＰアドレスとが一致したときに当該入力ＩＰパケットを前記おとり装置へ転送する、

ことを特徴とする請求項１記載の攻撃防御システム。

【請求項４】　前記ファイアウォール装置は、前記おとり装置へ転送した入力ＩＰパケットに関して前記攻撃検知手段が攻撃を検知したか否かに基づいて、前記振り分け条件を更新する振り分け条件更新手段をさらに有することを特徴とする請求項１記載の攻撃防御システム。

【請求項５】　前記フィルタリング条件管理手段は、前記おとり装置へ転送した入力ＩＰパケットのヘッダ情報に対応するフィルタリング条件を有効期限と共に設定し、前記入力ＩＰパケットに対応するフィルタリング条件の有効期限が超過している場合には、デフォルトのフィルタリング条件を前記パケットフィルタリング手段へ返すことを特徴とする請求項１記載の攻撃防御システム。

【請求項６】　前記フィルタリング条件管理手段は、

前記攻撃検知手段が攻撃を検知した際の攻撃カテゴリと当該入力ＩＰパケットのアドレス情報とに対応したフィルタリング条件を生成する条件生成手段と、

前記条件生成手段により生成されたフィルタリング条件に従って、フィルタリング条件を動的に更新するためのフィルタリング条件制御手段と、

を有することを特徴とする請求項１ないし５のいずれかに記載の攻撃防御システム。

【請求項７】　内部ネットワークと外部ネットワークとの境界に設置され、おとり装置およびファイアウォール装置を含む攻撃防御システムにおいて、

前記ファイアウォール装置は、

入力ＩＰパケットのヘッダ情報および振り分け条件に基づいて、当該入力ＩＰパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、

複数の入力ＩＰパケットにおける各送信元ＩＰアドレスの信頼度を管理するための信頼度管理手段と、

を有し、

前記転送先選択手段は、前記入力ＩＰパケットの送信元ＩＰアドレスに対する信頼度を前記信頼度管理手段から取得し、当該信頼度が前記振り分け条件を満たすか否かに応じて当該入力ＩＰパケットの転送先を決定することを特徴とする攻撃防御システム。

【請求項８】　前記信頼度管理手段は、ある信頼度が取得されるごとに、当該信頼度を更新することを特徴とする請求項７記載の攻撃防御システム。

【請求項９】　前記信頼度管理手段は、ある信頼度が取得されるごとに、当該信頼度に所定数を加算することを特徴とする請求項８記載の攻撃防御システム。

【請求項１０】　前記信頼度管理手段は、ある信頼度が取得されるごとに、当該信頼度に対応する入力ＩＰパケットのパケットサイズが大きくなるほど値が小さくなる変数を、当該信頼度に加算することを特徴とする請求項８記載の攻撃防御システム。

【請求項１１】　前記信頼度管理手段は、前記入力ＩＰパケットが予め定められたプロトコルのパケットである場合のみ信頼度の更新を実行することを特徴とする請求項８記載の攻撃防御システム。

【請求項１２】　前記信頼度管理手段は、

複数の入力ＩＰパケットにおける各送信元ＩＰアドレスの信頼度と当該信頼度の最終更新時刻とを格納するための第１信頼度格納手段と、

前記第１信頼度格納手段の内容の複製を格納するための第２信頼度格納手段と、

前記信頼度格納手段に格納されたある信頼度が前記転送先選択手段によって取得されるごとに、当該信頼度を更新する第１更新処理手段と、

前記第１信頼度格納手段の内容を定期的に複製して前記第２信頼度格納手段へ格納するための複製処理手段と、

前記第２信頼度格納手段に格納された信頼度の最終更新時刻を参照し、その最終更新時刻から所定期間が経過した信頼度を更新する第２更新処理手段と、

を有することを特徴とする請求項７記載の攻撃防御システム。

【請求項１３】　前記複製処理手段は、前記第１信頼度格納手段に格納された信頼度の最終更新時刻を参照し、その最終更新時刻から所定期間が経過した信頼度を有するエントリを前記第１信頼度格納手段から削除することを特徴とする請求項１２記載の攻撃防御システム。

【請求項１４】　前記第２更新処理手段は、前記最終更新時刻から所定期間

が経過した信頼度を所定値だけ低下させることを特徴とする請求項１２記載の攻撃防御システム。

【請求項１５】　前記第２更新処理手段は、前記最終更新時刻から所定期間が経過した信頼度を前記第２更新処理手段から削除することを特徴とする請求項１２記載の攻撃防御システム。

【請求項１６】　前記おとり装置は、前記ファイアウォール装置から転送された入力ＩＰパケットに対するサービスプロセスを実行することで攻撃の有無を検知する攻撃検知手段を有することを特徴とする請求項７記載の攻撃防御システム。

【請求項１７】　前記信頼度管理手段は、前記おとり装置へ転送した入力ＩＰパケットに関して前記攻撃検知手段が攻撃を検知したか否かに応じて、当該入力ＩＰパケットの送信元ＩＰアドレスの信頼度を更新することを特徴とする請求項１６記載の攻撃防御システム。

【請求項１８】　内部ネットワークと外部ネットワークとの境界に設置され、おとり装置およびファイアウォール装置を含む攻撃防御システムにおいて、

前記ファイアウォール装置は、

第１転送先選択手段と、

第２転送先選択手段と、

複数の入力ＩＰパケットにおける各送信元ＩＰアドレスの信頼度を管理するための信頼度管理手段と、

を有し、

前記第１転送先選択手段は、入力ＩＰパケットのヘッダ情報および第１所定条件に基づいて、当該入力ＩＰパケットを前記第２転送先選択手段および前記おとり装置のいずれかへ転送し、

前記第２転送先選択手段は、前記第１転送先選択手段から転送された前記入力ＩＰパケットの送信元ＩＰアドレスに対する信頼度を前記信頼度管理手段から取得し、当該信頼度が第２所定条件を満たすか否かに応じて当該入力ＩＰパケットの転送先を前記内部ネットワーク及び前記おとり装置のいずれかに決定する、

ことを特徴とする攻撃防御システム。

【請求項１９】　内部ネットワークと外部ネットワークとの境界に設置されたファイアウォール装置におけるおとり装置を用いた攻撃防御方法において、

ＩＰパケットのフィルタリング条件および振り分け条件を用意し、

入力ＩＰパケットのヘッダ情報および前記フィルタリング条件に基づいて、当該入力ＩＰパケットを受理するか否かを判定し、

受理された入力ＩＰパケットのヘッダ情報および前記振り分け条件に基づいて、当該入力ＩＰパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択し、

前記おとり装置に転送された入力ＩＰパケットに対するサービスプロセスを実行することで攻撃の有無を検知し、

攻撃を検知したか否かに基づいて、当該入力ＩＰパケットに対応するフィルタリング条件を管理する、

ステップを有することを特徴とする攻撃防御方法。

【請求項２０】　入力ＩＰパケットの前記ヘッダ情報は当該入力ＩＰパケットの送信元ＩＰアドレスおよび宛先ＩＰアドレスの少なくとも一方であり、

前記入力ＩＰパケットのヘッダ情報が前記振り分け条件を満たすか否かに依存して当該入力ＩＰパケットの転送先を決定することを特徴とする請求項１９記載の攻撃防御方法。

【請求項２１】　前記振り分け条件は、前記内部ネットワークで使用されていないＩＰアドレスからなる誘導リストであり、

前記入力ＩＰパケットの宛先ＩＰアドレスと前記誘導リスト内の未使用ＩＰアドレスとが一致したときに当該入力ＩＰパケットを前記おとり装置へ転送することを特徴とする請求項１９記載の攻撃防御方法。

【請求項２２】　攻撃を検知したか否かに基づいて、前記振り分け条件を更新するステップをさらに有することを特徴とする請求項１９記載の攻撃防御方法。

【請求項２３】　前記フィルタリング条件管理ステップは、

前記おとり装置へ転送した入力ＩＰパケットのヘッダ情報に対応するフィルタリング条件を有効期限と共に設定し、

前記入力ＩＰパケットに対応するフィルタリング条件の有効期限が超過している場合には、デフォルトのフィルタリング条件を設定する、

ことを特徴とする請求項１９記載の攻撃防御方法。

【請求項２４】　前記フィルタリング条件管理ステップは、

攻撃を検知した際の攻撃カテゴリと当該入力ＩＰパケットのアドレス情報とに対応したフィルタリング条件を生成し、

生成されたフィルタリング条件に従って、フィルタリング条件を動的に更新する、

ことを特徴とする請求項１９記載の攻撃防御方法。

【請求項２５】　内部ネットワークと外部ネットワークとの境界に設置されたファイアウォール装置におけるおとり装置を用いた攻撃防御方法において、

ＩＰパケットの振り分け条件を用意し、

複数の入力ＩＰパケットにおける各送信元ＩＰアドレスの信頼度を保持し、

入力ＩＰパケットの送信元ＩＰアドレスに対する信頼度が前記振り分け条件を満たすか否かに応じて、当該入力ＩＰパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する、

ステップを有することを特徴とする攻撃防御方法。

【請求項２６】　前記信頼度を保持するステップは、

複数の入力ＩＰパケットにおける各送信元ＩＰアドレスの信頼度と当該信頼度の最終更新時刻とをリアルタイム信頼度データベースに格納し、

前記リアルタイム信頼度データベースに格納されたある信頼度がアクセスされるごとに当該信頼度を更新し、

前記リアルタイム信頼度データベースの内容を定期的に複製して長期信頼度データベースに格納し、

前記長期信頼度データベースに格納された信頼度の最終更新時刻を参照し、その最終更新時刻から所定期間が経過した信頼度を更新する、

ステップを有することを特徴とする請求項２５記載の攻撃防御方法。

【請求項２７】　前記おとり装置において、前記ファイアウォール装置から転送された入力ＩＰパケットに対するサービスプロセスを実行することで攻撃の

有無を検知するステップをさらに有することを特徴とする請求項２５記載の攻撃防御方法。

【請求項２８】　攻撃が検知されたか否かに応じて、当該入力ＩＰパケットの送信元ＩＰアドレスの信頼度を更新するステップをさらに有することを特徴とする請求項２７記載の攻撃防御方法。

【請求項２９】　内部ネットワークと外部ネットワークとの境界に設置され、おとり装置に接続されたファイアウォール装置において、

入力ＩＰパケットのヘッダ情報およびフィルタリング条件に基づいて、当該入力ＩＰパケットを受理するか否かを判定するパケットフィルタリング手段と、

受理された入力ＩＰパケットのヘッダ情報および振り分け条件に基づいて、当該入力ＩＰパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、

前記おとり装置へ転送した入力ＩＰパケットに関して前記おとり装置が攻撃を検知したか否かに基づいて、当該入力ＩＰパケットに対応するフィルタリング条件を管理するフィルタリング条件管理手段と、

を有することを特徴とするファイアウォール装置。

【請求項３０】　内部ネットワークと外部ネットワークとの境界に設置され、おとり装置に接続されたファイアウォール装置において、

入力ＩＰパケットのヘッダ情報および振り分け条件に基づいて、当該入力ＩＰパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、

複数の入力ＩＰパケットにおける各送信元ＩＰアドレスの信頼度を管理するための信頼度管理手段と、

を有し、

前記転送先選択手段は、前記入力ＩＰパケットの送信元ＩＰアドレスに対する信頼度を前記信頼度管理手段から取得し、当該信頼度が前記振り分け条件を満たすか否かに応じて当該入力ＩＰパケットの転送先を決定することを特徴とするファイアウォール装置。

【請求項３１】　内部ネットワークと外部ネットワークとの境界に設置され

、おとり装置に接続されたファイアウォール装置において、

第１転送先選択手段と、

第２転送先選択手段と、

複数の入力ＩＰパケットにおける各送信元ＩＰアドレスの信頼度を管理するための信頼度管理手段と、

を有し、

前記第１転送先選択手段は、入力ＩＰパケットのヘッダ情報および第１所定条件に基づいて、当該入力ＩＰパケットを前記第２転送先選択手段および前記おとり装置のいずれかへ転送し、

前記第２転送先選択手段は、前記第１転送先選択手段から転送された前記入力ＩＰパケットの送信元ＩＰアドレスに対する信頼度を前記信頼度管理手段から取得し、当該信頼度が第２所定条件を満たすか否かに応じて当該入力ＩＰパケットの転送先を前記内部ネットワーク及び前記おとり装置のいずれかに決定することを特徴とするファイアウォール装置。

【請求項３２】　内部ネットワークと外部ネットワークとの境界に設置され、おとり装置に接続されたファイアウォール装置において、

入力ＩＰパケットのヘッダ情報およびフィルタリング条件に基づいて、当該入力ＩＰパケットを受理するか否かを判定するパケットフィルタリング手段と、

受理された入力ＩＰパケットのヘッダ情報および振り分け条件に基づいて、当該入力ＩＰパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、

複数の入力ＩＰパケットにおける各送信元ＩＰアドレスの信頼度を管理するための信頼度管理手段と、

前記おとり装置へ転送した入力ＩＰパケットに関して前記おとり装置が攻撃を検知したか否かに基づいて、当該入力ＩＰパケットに対応するフィルタリング条件を管理するフィルタリング条件管理手段と、

を有し、

前記転送先選択手段は、前記入力ＩＰパケットの送信元ＩＰアドレスに対する信頼度を前記信頼度管理手段から取得し、当該信頼度が前記振り分け条件を満た

すか否かに応じて当該入力ＩＰパケットの転送先を決定することを特徴とするファイアウォール装置。

【請求項３３】　前記おとり装置および前記ファイアウォール装置は単一ユニットに収容されていることを特徴とする請求項１、７および１８のいずれかに記載の攻撃防御システム。

【請求項３４】　前記転送先選択手段は、

入力ＩＰパケットを格納するパケットバッファと、

前記入力ＩＰパケットを前記内部ネットワークに転送し、宛先到達不能メッセージを受信するか否かを監視する監視手段と、

を有し、

前記監視手段が宛先到達不能メッセージを受信した場合、対応する入力ＩＰパケットを前記パケットバッファから前記おとり装置へ転送することを特徴とする請求項１記載の攻撃防御システム。

【請求項３５】　コンピュータに、内部ネットワークと外部ネットワークとの境界に設置されたファイアウォール装置におけるおとり装置を用いた攻撃防御システムを実装するためのプログラムにおいて、

ＩＰパケットのフィルタリング条件および振り分け条件を用意し、

入力ＩＰパケットのヘッダ情報および前記フィルタリング条件に基づいて、当該入力ＩＰパケットを受理するか否かを判定し、

受理された入力ＩＰパケットのヘッダ情報および前記振り分け条件に基づいて、当該入力ＩＰパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択し、

前記おとり装置に転送された入力ＩＰパケットに対するサービスプロセスを実行することで攻撃の有無を検知し、

攻撃を検知したか否かに基づいて、当該入力ＩＰパケットに対応するフィルタリング条件を管理する、

ステップを有することを特徴とする攻撃防御プログラム。

【請求項３６】　コンピュータに、内部ネットワークと外部ネットワークとの境界に設置されたファイアウォール装置におけるおとり装置を用いた攻撃防御

システムを実装するためのプログラムにおいて、

ＩＰパケットの振り分け条件を用意し、

複数の入力ＩＰパケットにおける各送信元ＩＰアドレスの信頼度を保持し、

入力ＩＰパケットの送信元ＩＰアドレスに対する信頼度が前記振り分け条件を満たすか否かに応じて、当該入力ＩＰパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する、

ステップを有することを特徴とする攻撃防御プログラム。

【請求項３７】　コンピュータに、内部ネットワークと外部ネットワークとの境界に設置されたおとり装置を用いたファイアウォール装置を実装するためのプログラムにおいて、

ＩＰパケットのフィルタリング条件および振り分け条件を用意し、

入力ＩＰパケットのヘッダ情報および前記フィルタリング条件に基づいて、当該入力ＩＰパケットを受理するか否かを判定し、

受理された入力ＩＰパケットのヘッダ情報および前記振り分け条件に基づいて、当該入力ＩＰパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択し、

前記おとり装置に対して、転送した入力ＩＰパケットに対するサービスプロセスを実行させることで攻撃の有無を検知させ、前記おとり装置が攻撃を検知したか否かに基づいて、当該入力ＩＰパケットに対応するフィルタリング条件を管理する、

ステップを有することを特徴とするプログラム。

【請求項３８】　コンピュータに、内部ネットワークと外部ネットワークとの境界に設置されたおとり装置を用いたファイアウォール装置を実装するためのプログラムにおいて、

ＩＰパケットの振り分け条件を用意し、

複数の入力ＩＰパケットにおける各送信元ＩＰアドレスの信頼度を保持し、

入力ＩＰパケットの送信元ＩＰアドレスに対する信頼度が前記振り分け条件を満たすか否かに応じて、当該入力ＩＰパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する、

ステップを有することを特徴とするプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明はコンピュータネットワークにおけるセキュリティ対策に係り、特に外部ネットワークからの攻撃に対して内部ネットワーク上の資源を保護するためのシステムおよび方法に関する。

【０００２】

【従来の技術】

従来、外部ネットワークからの攻撃に対する防御技術として、（１）ファイアウォール、（２）侵入検知システム、（３）おとりシステム、といった手法があった。

【０００３】

ファイアウォールの一例は、たとえば特開平８－４４６４２号公報に開示されている。外部のＩＰネットワークと内部のイーサネット（登録商標）との境界にファイアウォールを設置し、検査対象となるパケットを外部ネットワークから内部ネットワークに通過させてよいか否かを判定する。特に、ファイアウォールにパケットフィルタを設け、パケットのヘッダ情報（送信元アドレスや送信先アドレス）などの他、プロトコルの種別（ＴＣＰ／ＵＤＰ／ＨＴＴＰなど）や、データ内容（ペイロード）なども参照しながら、所定のルールに従って、パケットの通過可否を判定する。適切なルールを設定しておけば、例えば、外部ネットワーク一般に公開されているＷｅｂサーバなどに対してワームなどを含む不正なパケットが進入することを遮断できる。

【０００４】

侵入検知システムの一例は、たとえば特開２００１－３５０６７８号公報に開示されている。この従来の侵入検知システムは不正侵入判定ルール実行部を有し、アプリケーションごとの判定ルール、例えばWWWサーバ用不正侵入判定ルールやＭＡＩＬサーバ用不正侵入判定ルールを備えている。まず、ＩＰアドレステーブル取得部は、内部ネットワーク上を流れるパケットの送信元ＩＰアドレスも

しくは送信先ＩＰアドレスから、当該ＩＰアドレスを持つサーバにおいて現在動作中のアプリケーションを決定する。次に、不正侵入判定ルール実行部において、そのアプリケーションに応じた不正侵入判定ルールを実行し、当該パケットが不正であるか否かを判定する。こうすることにより、アプリケーションに依存したより精度の高い侵入検知が可能となる。

【０００５】

おとりシステムの第１例は、たとえば特開２０００－２６１４８３号公報に開示されている。この従来のおとりシステムは、ルータ１０の下に構築された内部ネットワーク上に、トラフィック監視装置、攻撃パターンおよび偽装サーバを備える。まず、トラフィック監視装置において、内部ネットワーク上を流れるパケットを監視しながら、特定の攻撃パターンに合致するものを不正パケットとして検出し、その識別情報（送信元ＩＰアドレス、送信先ＩＰアドレスなどを含む）をルータに通知する。次に、ルータでは、後に続く外部ネットワークからのパケットについて、検出した識別情報に合致するパケットをすべて偽装サーバに転送する。偽装サーバは、転送されたパケットを適切に解釈し、内部ネットワーク上の正規のサーバをまねた偽の応答パケットを生成し、先に不正パケットを送信したホストへ向けて、その偽の応答パケットを送信する。こうすることで、外部ネットワーク上に存在する攻撃者に、内部ネットワークに悪影響のない形で、攻撃を続けさせることができ、逆探知によって攻撃者の身元を明らかにすることができる。

【０００６】

おとりシステムの第２例は、たとえば特開２００２－７２３４公報に開示されている。この従来のおとりシステムは、内部ネットワークと外部ネットワーク（インターネット）との境界に、いわゆるゲートウェイとして、不正検出サーバと、おとりサーバと、を備える。外部ネットワークから内部ネットワークへ流れるパケットを不正検出サーバで監視し、例えば、当該パケットのペイロードについて所定のパターンマッチング処理を行うなどして、不正か否かを判定する。不正であると判定されたパケットには、その旨を示す特殊なマークを加えた上で、当該パケットをおとりサーバもしくは内部ネットワーク上の情報処理サーバへ転送

する。情報処理サーバへ不正パケットを転送する場合、予め情報処理サーバに不正回避処理部を持たせておき、特殊なマークのあるパケットを受信した際には、さらにおとりサーバへ当該パケットを転送するようにしておく。いずれにせよ、不正検出サーバで検出された不正パケットは、最終的におとりサーバへ到達する。その後、おとりサーバでは、偽の応答パケットを生成し、不正パケットの送信元ホストに向けて、当該応答パケットを送信する。こうすることで、不正と判定されたパケットは全ておとりサーバに閉じ込めることができる。

【０００７】

さらに、おとりシステムの第３例は、たとえば特開平０９－２２４０５３公報に記載されている。この従来のおとりシステムは、公衆ネットワーク（インターネット）と、プライベートネットワーク（内部ネットワーク）との境界に、スクリーン・システムおよび代行ネットワークを備える。スクリーン・システムは、自身に接続される各ネットワークからの着信パケットについて、パケットのヘッダに記載される情報や着信履歴など基にしたスクリーン基準に従い、フィルタリングを行う。ただし、スクリーン・システムの通信インタフェースはＩＰアドレスをもたず、ｔｒａｃｅｒｏｕｔｅなどを用いた探索から自身を隠蔽することを特徴の１つとする。もう１つの特徴として、プライベートネットワークに向かう着信パケットについて、代行ネットワークに経路を変更することもできる。代行ネットワーク上には０台以上の代行ホストが設けられ、プライベートネットワーク上にあるホストの代理として動作させることもできる。こうすることで、公衆ネットワークからの攻撃からプライベートネットワークを保護できる。

【０００８】

【発明が解決しようとする課題】

しかしながら、従来の技術のいずれも、以下に挙げるような問題点を持つ。

【０００９】

第１の問題点は、外部ネットワーク上の攻撃ホストと内部ネットワーク上のサーバとの間で、ＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）やＩＰＳｅｃ（ＲＦＣ２４０１記載）などの通信路暗号化技術が用いられた場合に、攻撃を有効に検知または防御できないということである。その理由は、攻撃検知のため

の主要なデータ（ペイロードなど）が暗号化されており参照できないためである。

【００１０】

第２の問題点は、攻撃検知部のパフォーマンスが、近年のネットワークの高速化に追随しきれず、検査から漏れるパケットが存在したり、ネットワークの高速性を損なったりする点にある。その理由は、攻撃検知の精度を向上するには、より多彩な、あるいはより複雑な判定ルールの実行が必要であるが、一方、ネットワークの高速化により、検査対象となるパケット量が飛躍的に増加しているためである。

【００１１】

また、上述した侵入検知システムやおとりシステムの第１例では、少なくとも１つの不正パケットが、内部ネットワーク上の保護すべきサーバに到達してしまう。その理由は、攻撃検知部が検査を行うのは、パケットのコピーでしかなく、当該パケットが不正と判定された場合でも、その内部ネットワーク上のパケット流通を遮断できないためである。

【００１２】

さらに、上記おとりシステムの第３例では、インターネットから到来したパケットを代行ネットワークに経路変更させる条件および方法については検討されていない。このために、正確にパケットを振り分けることができず、正常なアクセスが代行ネットワークへ、異常なアクセスが内部ネットワークへ導かれる可能性がある。

【００１３】

本発明の目的は、通信路暗号化技術を用いた通信システムに対しても、外部ネットワークからの攻撃を有効に防御できる攻撃防御システムおよび方法ならびにファイアウォール装置を提供することにある。

【００１４】

本発明の他の目的は、高速ネットワーク環境に対応できる攻撃防御システムおよび方法ならびにファイアウォール装置を提供することにある。

【００１５】

本発明のさらに他の目的は、保護すべきサーバに向けられた不正パケットを確実に遮断できる攻撃防御システムおよび方法ならびにファイアウォール装置を提供することにある。

【００１６】

【課題を解決するための手段】

本発明の第１の観点によれば、おとり装置およびファイアウォール装置を含む攻撃防御システムが内部ネットワークと外部ネットワークとの境界に設置され、おとり装置はファイアウォール装置から転送された入力ＩＰパケットに対するサービスプロセスを実行することで攻撃の有無を検知する攻撃検知手段を有し、ファイアウォール装置は、入力ＩＰパケットのヘッダ情報およびフィルタリング条件に基づいて当該入力ＩＰパケットを受理するか否かを判定するパケットフィルタリング手段と、受理された入力ＩＰパケットのヘッダ情報および振り分け条件に基づいて当該入力ＩＰパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、前記おとり装置へ転送した入力ＩＰパケットに関して前記攻撃検知手段が攻撃を検知したか否かに基づいて当該入力ＩＰパケットに対応するフィルタリング条件を管理するフィルタリング条件管理手段と、を有する、ことを特徴とする。

【００１７】

本発明の第２の観点によれば、ファイアウォール装置は、入力ＩＰパケットのヘッダ情報および振り分け条件に基づいて当該入力ＩＰパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、複数の入力ＩＰパケットにおける各送信元ＩＰアドレスの信頼度を管理するための信頼度管理手段と、を有し、前記転送先選択手段は、前記入力ＩＰパケットの送信元ＩＰアドレスに対する信頼度を前記信頼度管理手段から取得し、当該信頼度が前記振り分け条件を満たすか否かに応じて当該入力ＩＰパケットの転送先を決定することを特徴とする。

【００１８】

本発明による攻撃防御方法は、入力ＩＰパケットのヘッダ情報およびフィルタリング条件に基づいて、当該入力ＩＰパケットの受理および廃棄のいずれかを実

行し、受理された入力ＩＰパケットのヘッダ情報および振り分け条件に基づいて、当該入力ＩＰパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択し、前記入力ＩＰパケットが前記おとり装置へ転送されると、当該入力ＩＰパケットに対するサービスプロセスを実行し、前記サービスプロセスの実行状況を監視しながら、所定の攻撃カテゴリと関連づけられたルールに違反するか否かを判定することで攻撃の有無を検知し、前記入力ＩＰパケットに関して攻撃を検知したか否かに応じて、当該入力ＩＰパケットのヘッダ情報に対応するフィルタリング条件を設定し、入力したＩＰパケットのヘッダ情報に対応するフィルタリング条件に従ってパケットフィルタリングを実行する、ステップを有することを特徴とする。

【００１９】

望ましくは、本発明によるファイアウォール装置は、入力ＩＰパケットのヘッダ情報およびフィルタリング条件に基づいて当該入力ＩＰパケットを受理するか否かを判定するパケットフィルタリング手段と、受理された入力ＩＰパケットのヘッダ情報および振り分け条件に基づいて当該入力ＩＰパケットの転送先として前記内部ネットワークおよび前記おとり装置のいずれかを選択する転送先選択手段と、複数の入力ＩＰパケットにおける各送信元ＩＰアドレスの信頼度を管理するための信頼度管理手段と、前記おとり装置へ転送した入力ＩＰパケットに関して前記おとり装置が攻撃を検知したか否かに基づいて当該入力ＩＰパケットに対応するフィルタリング条件を管理するフィルタリング条件管理手段と、を有し、前記転送先選択手段は、前記入力ＩＰパケットの送信元ＩＰアドレスに対する信頼度を前記信頼度管理手段から取得し、当該信頼度が前記振り分け条件を満たすか否かに応じて当該入力ＩＰパケットの転送先を決定することを特徴とする。

【００２０】

【発明の実施の形態】

（ネットワーク構成）

図１は、本発明による攻撃防御システムの概略的ブロック図である。本発明による攻撃防御システムは、基本的に、ファイアウォール装置１およびおとり装置２を有し、インターネット３と内部ネットワーク４との境界にファイアウォール

装置１が設置されている。内部ネットワーク４は、WWW（World-Wide Web）などのサービスを提供する１個以上のサーバ装置４０１を含む。ここではインターネット３に攻撃元ホスト３０１が想定されている。

【００２１】

ファイアウォール装置１は、通常の正規のパケットであれば、これを通過させて内部ネットワーク４へ送付し、不正パケットあるいは不審なパケットであれば、おとり装置２へ誘導する。おとり装置２は攻撃の有無を検知し、攻撃を検知した場合にはアラートをファイアウォール装置１へ出力する。また、不正パケットに対する偽の応答パケットを生成してファイアウォール装置１へ返してもよい。ファイアウォール装置１はその偽の応答パケットを不正パケットの送信元である攻撃元ホスト３０１へ送信する。

【００２２】

（第１実施形態）

１．１）構成

図２は、本発明の第１実施形態による攻撃防御システムのファイアウォール装置１およびおとり装置２の構成を示すブロック図である。ファイアウォール装置１は、外部通信インタフェース１００でインターネット３と接続され、第１の内部通信インタフェース１０４で内部ネットワーク４と接続される。

【００２３】

パケットフィルタ１０１は、外部通信インタフェース１００および誘導部１０３の間に接続され、アクセス制御リスト管理部１０２から取得したアクセス制御ルールに従ってパケットフィルタリングを行う。後述するように、外部通信インタフェース１００または誘導部１０３の一方から受け取ったＩＰパケットを他方へ転送し、あるいは転送せずに廃棄する。

【００２４】

パケットフィルタ１０１で受理されたパケットは誘導部１０３へ送られ、誘導部１０３は、後述する誘導リスト（図５）を参照し、パケットフィルタ１０１から入力したＩＰパケットの宛先ＩＰアドレスに応じて当該パケットを第１の内部通信インタフェース１０４および第２の内部通信インタフェース１０５のいずれ

かへ誘導する。逆に、第１の内部通信インタフェース１０４または第２の内部通信インタフェース１０５からインターネット３に向かうＩＰパケットをパケットフィルタ１０１に転送する。

【００２５】

第１の内部通信インタフェース１０４は、誘導部１０３から入力したＩＰパケットを内部ネットワーク４に伝達し、内部ネットワーク４からインターネット３に向かうＩＰパケットを誘導部１０３へ伝達する。第２の内部通信インタフェース１０５は、誘導部１０３によって誘導されたＩＰパケットをおとり装置２に伝達し、おとり装置２からインターネット３に向かうＩＰパケットを誘導部１０３に伝達する。

【００２６】

おとり装置２は、プロセッサ２０１と攻撃検知部２０２とを含む。プロセッサ２０１は、WWWやＴｅｌｎｅｔなどのネットワークサービスを提供するプロセスを実行しながら、当該プロセスの状況を攻撃検知部２０２へ随時伝達する。攻撃検知部２０２は、プロセッサ２０１から入力されるプロセス状況を監視しながら、攻撃の有無を検査し、攻撃が認められた場合には攻撃内容を報告するためのアラートを生成しファイアウォール装置１へ送出する。

【００２７】

制御インタフェース１０６を通してアラートを入力すると、防御ルール判定部１０７は、アラートの内容に従ってアクセス制御リスト管理部１０２のアクセス制御リストの更新等を指示する。

【００２８】

図３は、図２のファイアウォール装置１におけるアクセス制御リスト管理部１０２の模式的構成図である。アクセス制御リスト管理部１０２は、アクセス制御リストデータベース１０２１、検索部１０２２および更新処理部１０２３を有する。アクセス制御リストデータベース１０２１は、少なくとも「ソースＩＰアドレス」、「ディスティネーションＩＰアドレス」および「フィルタ処理方法」といったフィールドを有するエントリ（アドレス制御ルール）の集合を検索可能に保持する。検索部１０２２は、パケットフィルタ１０１からＩＰアドレスなどを

含む問い合わせ（ＲＱ）を受けると、アクセス制御リストデータベース１０２１から対応するアクセス制御ルールを検索してパケットフィルタ１０１へ返す。更新処理部１０２３は、防御ルール判定部１０７から入力した更新用アクセス制御ルールに従ってアクセス制御リストデータベース１０２１の内容を更新（追加／修正）する。

【００２９】

図４は、アクセス制御リストデータベース１０２１の内容を例示した模式図である。アクセス制御リストデータベース１０２１には複数のアクセス制御ルールが所定の規則に従って格納される。各アクセス制御ルールは、図４に示すように、ソースＩＰアドレス（ＳＲＣ）やディスティネーションＩＰアドレス（ＤＳＴ）などのルール適合条件と、パケットの受理（ＡＣＣＥＰＴ）、拒否（ＤＥＮＹ）、廃棄（ＤＲＯＰ）などの所定の処理方法（ＰＲＯＣ）を示す識別子との組からなる。アクセス制御ルールは一般に複数設定されるので、その集合をアクセス制御リストデータベース１０２１で保持しておく。図４において、アスタリスク（＊）は任意のアドレスを示し、パケットフィルタ処理の“ＡＣＣＥＰＴ”はパケットの受理、“ＤＥＮＹ”はＩＣＭＰエラー通知をするパケット拒否、“ＤＲＯＰ”はＩＣＭＰエラー通知をしないパケット廃棄をそれぞれ示す。

【００３０】

図５は、誘導部１０３に設けられた誘導リストの一例を示す模式図である。誘導部１０３には、予め１つ以上のＩＰアドレスからなる誘導リストが保持されている。本実施例の誘導リストでは、内部ネットワーク４の未使用ＩＰアドレスが列挙されている。後述するように、未使用であるはずのＩＰアドレスを宛先とするパケットは、不審パケットである可能性が高い。

【００３１】

図６は、防御ルール判定部１０７に保持されている防御ルールスクリプトを例示した模式図である。詳しくは後述するが、防御ルール判定部１０７は、探査（RECON）、侵入(INTRUSION)、破壊(DESTRUCTION)などの攻撃種別ごとに、防御ルールを列挙し、例えばファイル形式で保持している。防御ルールは、所定の攻撃カテゴリに１対１対応する形式で、１つのアクセス制御ルールの雛型を指定する

記述が用いられる。例えば、

ＩＮＴＲＵＳＩＯＮ：（ＳＲＣ：＄｛ＳＯＵＲＣＥ＿ＩＰ＿ＡＤＤＲＥＳＳ｝，ＤＳＴ：＊，ＰＲＯＣ：ＤＲＯＰ）

といった記述が行ごとに攻撃種別ごとに列挙されている。この記述のうち「＄｛ＳＯＵＲＣＥ＿ＩＰ＿ＡＤＤＲＥＳＳ｝」の部分が、後述するように、おとり装置２からのアラートに記載された情報（攻撃パケットのソースＩＰアドレス）で置き換えられる変数である。

【００３２】

１．２）動作

１．２．１）パケットフィルタリング

図７は、本発明の第１実施形態による攻撃防御システムの動作を示すフローチャートである。まず、ファイアウォール装置１において、インターネット３から内部ネットワーク４へ向けたＩＰパケットを外部通信インタフェース１００で捉えた後、当該ＩＰパケットをパケットフィルタ１０１へ転送する（ステップＡ１）。

【００３３】

次に、パケットフィルタ１０１は、当該ＩＰパケットのヘッダを参照し、そこに記載されているソースＩＰアドレスやディスティネーションＩＰアドレスなどの情報をアクセス制御リスト管理部１０２へ出力する。アクセス制御リスト管理部１０２は、上述したように、入力したＩＰアドレスを用いてアクセス制御リストデータベース１０２１を検索し、ヒットした最初のアクセス制御ルールをパケットフィルタ１０１へ返す。アクセス制御ルールを取得すると、パケットフィルタ１０１は、その処理方法に従って、当該ＩＰパケットを受理または廃棄する（ステップＡ２）。ＩＰパケットを受理した場合は、当該ＩＰパケットを誘導部１０３へ転送し、廃棄した場合は、直ちに次のパケットの処理へと制御を移す。

【００３４】

アクセス制御リスト管理部１０２におけるアクセス制御ルールの検索において、パケットフィルタ１０１から入力したソースＩＰアドレスを検索部１０２２が受け取ると、検索部１０２２は個々のアクセス制御ルールの適合条件と入力した

ソースＩＰアドレスとを照合し、適合条件を満たす最初のアクセス制御ルールを抽出し、パケットフィルタ１０１へ返す。

【００３５】

１．２．２）パケット誘導

次に、誘導部１０３では、パケットフィルタ１０１で受理されたＩＰパケットに対して、そのディスティネーションＩＰアドレスと予め設けられた誘導リストとを参照し、転送すべき内部通信インタフェース（１０４あるいは１０５）を決定する（ステップＡ３）。具体的には、図５に示すような誘導リストと、ディスティネーションＩＰアドレスとを照合し、合致するものがある場合には、第２の内部通信インタフェース１０５を介して当該ＩＰパケットをおとり装置２へ転送する。合致するものがない場合には、第１の内部通信インタフェース１０４を介して内部ネットワーク４へ当該ＩＰパケットを伝達する。

【００３６】

ＩＰパケットが内部ネットワーク４へ伝達された場合には、当該ＩＰパケットは内部ネットワーク４上の適切なサーバ装置３０１に到達し、所定のサービスを提供するための処理が行われる（ステップＡ４）。

【００３７】

一方、ＩＰパケットがおとり装置２へ伝達された場合には、そのプロセッサ２０１において、偽のサービスを提供するための処理を行いながら、入力データの内容や処理状況を逐次的に攻撃検知部２０２へ通知する（ステップＡ５）。この際、おとり装置２は、ファイアウォール装置１から伝達されたＩＰパケットを、そのディスティネーションＩＰアドレスの如何を問わず、受信することができる。具体的には、おとり装置２に複数のＩＰアドレスを割り当てられるような工夫を施してもよいし、あるいは図８に示すように、予め誘導部１０３にアドレス変換部１０３１を備えておき、入力ＩＰパケットのディスティネーションＩＰアドレスをおとり装置２のＩＰアドレスに書き換えた上で、おとり装置２に当該ＩＰパケットを伝達するような方法を用いてもよい。

【００３８】

１．２．３）偽サービス提供

ＩＰパケットを受信後、おとり装置２は、偽のサービスとして、WWWやＴｅｌｎｅｔなど１つ以上の任意のものを提供する。ただし、本実施形態においては、通信プロトコルさえ適切に処理すれば十分であり、実際のサービスで行われるような、ファイルシステムへのアクセスやデータベース処理などは一切行わなくともよい。具体的には、例えば、Ｔｅｌｎｅｔサービスの場合であれば、Ｌｏｇｉｎ／Ｐａｓｓｗｏｒｄプロンプトへの任意の入力に対して、すべてログインを許可し、ユーザに偽のメッセージを応答するような偽装シェルを起動するようにしてもよい。

【００３９】

１．２．４）攻撃検知

次に、おとり装置２の攻撃検知部２０２では、プロセッサ２０１から通知される処理状況について、正常動作定義との照合を行い、攻撃の有無を判定する（ステップＡ６）。正常動作定義とは、おとり装置２上で提供されるサービスの正しい振舞いに関する条件の集合である。具体的には、例えば、WWWサービスに対して「WWWサービスに対応するプロセスは自ら他のサーバ装置にネットワークアクセスをすることはない」というような条件や、「／ｕｓｒ／ｌｏｃａｌ／ｗｗｗ／ｌｏｇｓディレクトリ以外にファイルを書き込むことはない」というような条件などの集合である（詳しくは、図１２参照）。これらの各条件と通知された処理状況とを照合し、合致しない条件を少なくとも１つ検出した際に、「攻撃あり」と判断する。

【００４０】

攻撃を検出した際、違反した条件の意味に応じて、攻撃種別を決定し、その結果をアラートとしてファイアウォール装置１へ送信する（ステップＡ７）。

【００４１】

攻撃種別とは、当該攻撃に対する防御方法を導出するに十分な分類をいい、例えば、

・「探査」：ポートスキャンやバナー攻撃などのいわゆる「フィンガープリンティング」

・「侵入」：トロイの木馬やアカウントの追加などのバックドア設置

・「破壊」：Ｐｉｎｇ　Ｏｆ　Ｄｅａｔｈなどのサービス不能攻撃

などを指す。その方法の一例として、正常動作定義の中の各条件について、違反時に想定される攻撃種別を予め併記しておけばよい。例えば、前記した「／ｕｓｒ／ｌｏｃａｌ／ｗｗｗ／ｌｏｇｓディレクトリ以外にファイルを書き込むことはない」という条件に違反するような攻撃については、バックドア設置の可能性が高いので、「侵入」を示す識別子を当該条件に併記しておく。

【００４２】

１．２．５）アクセス制御リストの更新

最後に、ファイアウォール装置１における防御ルール判定部１０７では、制御インタフェース１０６を介しておとり装置２から受信したアラートを参照し、防御ルールを用いてアクセス制御ルールを生成し、アクセス制御リスト管理部１０２へ当該アクセス制御ルールを追加するよう指示する（ステップＡ８）。

【００４３】

具体的には、防御ルール判定部１０７に、予め攻撃種別ごとに、図６のような防御ルールスクリプトを設定しておく。防御ルールスクリプトには、図６のような書式によって、攻撃種別と更新すべきアクセス制御ルールのひな型との組を記述する。アクセス制御ルールのひな型には、アラートに記載された情報を挿入するための変数が記述できる。たとえば、

（ＳＲＣ：＄｛ＳＯＵＲＣＥ＿ＩＰ＿ＡＤＤＲＥＳＳ｝，ＤＳＴ：１．２．３．４，ＰＲＯＣ：ＤＲＯＰ）

と記述されている場合、「＄｛ＳＯＵＲＣＥ＿ＩＰ＿ＡＤＤＲＥＳＳ｝」の箇所は、アラートに記載されたソースＩＰアドレスで置換され、

（ＳＲＣ：１２．３４．５６．７８，ＤＳＴ：１．２．３．４，ＰＲＯＣ：ＤＲＯＰ）

といった完全な形式のアクセス制御ルールに変換される。そして、当該アクセス制御ルールは、アクセス制御リスト管理部１０２内の更新処理部１０２３へ伝達され、アクセス制御リストデータベース１０２１に適切に追加される。同じソースＩＰアドレスおよびディスティネーションＩＰアドレスの組をもつアクセス制御ルールが既にアクセス制御リストデータベース１０２１に登録されている場合

には、更新処理部１０２３は、新たに追加されたアクセス制御ルールが有効になるように適切にアクセス制御リストデータベース１０２１を更新する。たとえば、アクセス制御リストデータベース１０２１の検索スキャン方向の先頭に位置するように追加される。

【００４４】

１．３）効果

第１実施形態のファイアウォール装置１では、誘導部１０３において、誘導リストとディスティネーションＩＰアドレスとの照合結果により、おとり装置２へ誘導する方法を用いている。このために、内部ネットワーク４の既存の構成を一切変更することなく、おとり装置２を設置可能となる。さらに、誘導リストに含めるＩＰアドレスとして、内部ネットワーク４における未使用のＩＰアドレス群を記載することで、１台のおとり装置２で、内部ネットワーク４上に複数のおとり装置２を設置するのと同じ効果が得られる。

【００４５】

通常、「ＣｏｄｅＲｅｄ」や「Ｎｉｍｄａ」などの自動感染機能をもつワームは、ある連続したＩＰアドレスの区間からランダムにＩＰアドレスを選択しながら、感染を試みるよう動作する。したがって、おとり装置２は設置台数が多ければ多いほど検知の確率が高くなる。本実施形態では、図５に示すような誘導リストの作成でその効果を得ることができる。

【００４６】

また、ファイアウォール装置１の外部通信インタフェース１００に割り当てられたＩＰアドレスを誘導リストに含めることで、インターネット３側からは、ファイルウォール装置１とおとり装置２との見分けがつかなくなる。一般に、インターネット３からの攻撃は、ファイアウォールの発見から始まるので、本実施形態はファイアウォール装置１を「隠す」という効果をもつ。

【００４７】

１．４）具体例

図９～図１１は第１実施形態の具体的動作例を説明するためのネットワーク構成図であり、図１２はおとり装置２における攻撃検知動作を説明するための模式

図である。

【００４８】

図９に示すように、インターネット３上に攻撃元ホスト３０１（ＩＰアドレス：１２．３４．５６．７８）があり、内部ネットワーク４上にインターネットサーバ装置４０１がありものとする。さらに、インターネット３と内部ネットワーク４との境界にファイアウォール装置１が設置され、標準的なポート番号であるＴＣＰ８０番ポートにおいてWWWサービスを提供するおとり装置２が設置されているものとする。また、内部ネットワーク４のネットワークアドレスとして、「１．２．３．ｘ／２４」が用いられており、サーバ装置４０１には「１．２．３．４」というＩＰアドレスが設定されているものとする。

【００４９】

今、攻撃元ホスト３０１はWWWサービスに対する自動感染機能をもつワームに感染しており、当該ワームが次の感染先として、内部ネットワーク４に対応する「１．２．３．ｘ／２４」に狙いを定め、かつ「１．２．３．１」を第１の感染先として選択したものとする。このとき、攻撃元ホスト３０１から内部ネットワーク４に向けて、ＳＹＮパケット（ソースＩＰアドレス：１２．３４．５６．７８、ディスティネーションＩＰアドレス：１．２．３．１）が送信される。

【００５０】

当該ＳＹＮパケットは、まず、ファイアウォール装置１の外部通信インタフェース１００に到達した後、ただちにパケットフィルタ１０１に伝達される。パケットフィルタ１０１では、アクセス制御リスト管理部１０２に対して、少なくとも当該ＳＹＮパケットのソースＩＰアドレス「１２．３４．５６．７８」とディスティネーションＩＰアドレス「１．２．３．１」とを出力する。この他、アクセス制御ルールの粒度を高めるために、プロトコル番号「６」（ＴＣＰを示す）や、ポート番号「８０」などを出力できるようにしてもよいが、本実施例では例としてソースＩＰアドレスとディスティネーションＩＰアドレスだけを入力するものとする。

【００５１】

アクセス制御リスト管理部１０２におけるアクセス制御リストデータベース１

０２１は、例えば、図４のようなテキスト形式で記述されたアクセス制御リストを保持しているものとする。上述したように、各行は１つのアクセス制御ルールを示しており、ＳＲＣフィールドとＤＳＴフィールドとの組が適合条件を、ＰＲＯＣフィールドがフィルタ処理方法をそれぞれ示す。

【００５２】

検索部１０２２では、パケットフィルタ１０１から入力として与えられたソースＩＰアドレス「１２．３４．５６．７８」およびディスティネーションＩＰアドレス「１．２．３．１」との組を検索キーとして、適切なアクセス制御ルールを抽出するために、アクセス制御リストデータベースの先頭行から順に各アクセス制御ルールを参照しながら、各ルールの適合条件と前記入力との比較を行い、適合する最初のアクセス制御ルールを抽出する。この時点では、「（ＳＲＣ：＊，ＤＳＴ：１．２．３．１，ＰＲＯＣ：ＡＣＣＥＰＴ）」（「ＰＲＯＣ：ＡＣＣＥＰＴ」は入力ＩＰパケットの受理を示す）というアクセス制御ルールが適合したとする。このとき、検索部１０２２は、「（ＳＲＣ：１２．３４．５６．７８，ＤＳＴ：１．２．３．１，ＰＲＯＣ：ＡＣＣＥＰＴ）」をパケットフィルタ１０１に返す。

【００５３】

アクセス制御ルールを受け取ったパケットフィルタ１０１は、当該ルールのＰＲＯＣフィールドを参照し、「ＡＣＣＥＰＴ」であることを確認すると、ただちに入力ＩＰパケットを後段の誘導部１０３へと伝達する。

【００５４】

続いて、誘導部１０３では、受け取った入力ＩＰパケットのディスティネーションＩＰアドレスと内部的に保持する誘導リストとを参照し、次の転送先を決定する。本実施例では、誘導リスト内に内部ネットワーク４の未使用ＩＰアドレスが列挙されており、その１つが「１．２．３．１」であるものとする。この場合、誘導部１０３は、入力ＩＰパケットのディスティネーションＩＰアドレス「１．２．３．１」が誘導リストに記載されているのを確認した後、当該入力ＩＰパケットをおとり装置２が接続されている第２の内部通信インタフェース１０５へと伝達する（図１０参照）。

【００５５】

おとり装置２は、第２の内部通信インタフェース１０５へ伝達された全てのＩＰパケットを、そのディスティネーションＩＰアドレスの如何によらず受け付ける。おとり装置２では偽のWWWサービスが稼動しており、ワームが発したＳＹＮパケットを受け付けると共に、ＳＹＮ－ＡＣＫパケットをそのソースＩＰアドレス（すなわち攻撃元ホスト３０１）へ向けて出力する。

【００５６】

これ以降、ファイアウォール装置１で同様の処理が繰り返されて、攻撃元ホスト３０１とおとり装置２との間でＴＣＰ接続確立のための通信と、ワーム感染のための（不正な）通信が行われる。

【００５７】

おとり装置２では、プロセッサ２０１でWWWサービスを攻撃元ホスト３０１へ提供する。それと並行して、プロセッサ２０１は、ファイルアクセスやネットワークアクセスなどの動作状況を、攻撃検知部２０２へ逐次的に通知する。攻撃元ホスト３０１上のワームは、おとり装置２上のWWWサービスに対して、感染を試みる。具体的には、例えば、

「ＧＥＴ　／ｄｅｆａｕｌｔ．ｉｄａ？ＮＮＮＮＮＮＮＮＮＮＮＮ（２００バイト程度の繰り返し）…％ｕ００００％ｕ００＝ａ　ＨＴＴＰ／１．１」といった文字列から始まる、非常に大きなメッセージをWWWサービスに対して入力し、いわゆる「バッファオーバーフロー」を引き起こすことで、任意のコマンドを実行しようとする。この際、一般的なワームは、ワーム自身のコードをディスク上のシステム領域にコピーした後、当該コードを実行するようなコマンドを発行する。したがって、ワームの侵入時に、プロセッサ２０１は、システム領域へファイルの書き出しが行われたこと、あるいは、当該ファイルの実行が行われたことを攻撃検知部２０２に伝達することになる。このとき、同時に、おとり装置２が受け付けた入力ＩＰパケットのコピーも併せて伝達する。

【００５８】

攻撃検知部２０２は、予めプロセッサ２０１上のWWWサービスの適正な動作に関する情報を、正常動作定義ファイルとして保持している。正常動作定義ファ

イルは、例えば、図１２のような形式で記述されており、ファイルの読み込み、書き出し、実行などに関する条件が列挙されている。

【００５９】

ここで、前記ワームが自身のコピーを書き出す箇所を「Ｃ：￥Ｗｉｎｄｏｗｓ」ディレクトリだとすると、その動作は図１２に示す正常動作定義ファイル内の第２番目の条件である

「ＷＲＩＴＥ，Ｃ：￥Ｉｎｅｔｐｕｂ￥ｗｗｗｒｏｏｔ￥＿ｖｔｉ＿ｌｏｇ￥＊；ＩＮＴＲＵＳＩＯＮ」（「Ｃ：￥Ｉｎｅｔｐｕｂ￥ｗｗｗｒｏｏｔ￥＿ｖｔｉ＿ｌｏｇディレクトリ以下にのみファイル書き出しを行う」の意）

に違反する。このとき、攻撃検知部２０２は、当該条件の「；」以下を参照し、ＩＮＴＲＵＳＩＯＮ（侵入）カテゴリに属する攻撃があったと判定する。

【００６０】

続いて、攻撃検知部２０２は、少なくとも、入力ＩＰパケットに含まれるソースＩＰアドレスと、検出された攻撃のカテゴリが「ＩＮＴＲＵＳＩＯＮ」であることを知らせるためのアラートを生成し、ファイアウォール装置１の制御インタフェース１０６へ伝達する（図１１参照）。

【００６１】

制御インタフェース１０６で受信されたアラートは防御ルール判定部１０７へ伝達される。アラートの入力を受けた防御ルール判定部１０７は、上述したように、防御ルールを列挙したスクリプトを、例えばファイル形式で保持している。各防御ルールは、所定の各攻撃カテゴリに１対１対応する形式で、１つのアクセス制御ルールのひな型が指定されている（図６参照）。

【００６２】

具体的には、例えば、

ＩＮＴＲＵＳＩＯＮ：（ＳＲＣ：＄｛ＳＯＵＲＣＥ＿ＩＰ＿ＡＤＤＲＥＳＳ｝，ＤＳＴ：＊，ＰＲＯＣ：ＤＲＯＰ）　　・・・（１）

といった記述が行ごとに列挙されている。ここで、アラートの入力を受けた防御ルール判定部１０７は、防御ルールの定義ファイルを行ごとに参照し、「ＩＮＴＲＵＳＩＯＮ」カテゴリに対応する防御ルールである式（１）を抽出する。そし

て、アクセス制御ルールの雛型に対して、当該アラートに記載されたソースＩＰアドレス「１２．３４．５６．７８」（すなわち攻撃元ホストのＩＰアドレス）によって、「＄｛ＳＯＵＲＣＥ＿ＩＰ＿ＡＤＤＲＥＳＳ｝」を置換し、

（ＳＲＣ：１２．３４．５６．７８，ＤＳＴ：＊，ＰＲＯＣ：ＤＲＯＰ）

・・・（２）

というアクセス制御ルールを生成する（「ＤＳＴ：＊」は任意のディスティネーションＩＰアドレスに適合する）。そして、当該アクセス制御ルールをアクセス制御リスト管理部１０２へ伝達する。

【００６３】

アクセス制御リスト管理部１０２では、防御ルール判定部１０７からのアクセス制御ルールの入力について更新処理部１０２３で処理する。更新処理部１０２３では、式（２）で示されるアクセス制御ルールを、アクセス制御リストデータベース１０２１に伝達し、その追加を指示する。アクセス制御リストデータベース１０２１では、式（２）で示されるアクセス制御ルールを追加するように更新処理を行う。その際、アクセス制御リストデータベース１０２１は、それ以降の検索処理が最近の更新結果を反映するように適切に更新処理を行う。例えば、図４のようなテキスト形式で記述されたアクセス制御リストを用い、先頭行から順に検索処理を行うような場合であれば、式（２）を先頭行に追加すればよい。つまり、たとえ次式（３）といったようなアクセス制御ルールが予め設定されていたとしても、

（ＳＲＣ：１２．３４．５６．７８，ＤＳＴ：＊，ＰＲＯＣ：ＡＣＣＥＰＴ）

・・・（３）

当該更新処理以降、検索部１０２２がソースＩＰアドレス「１２．３４．５６．７８」を含む入力を受けた場合には、式（３）ではなく式（２）を検索結果として出力する（図１３参照）。

【００６４】

次に、攻撃元ホスト３０１上のワームが次の攻撃先として、「１．２．３．４」を選択したものとする。しかる後、先の攻撃と同様に、内部ネットワーク４上のサーバ装置４０１に向けたＳＹＮパケットがファイアウォール装置１に到達す

る。その場合、当該ＳＹＮパケットの入力をうけたパケットフィルタ１０１は、アクセス制御リスト管理部１０２から適合するアクセス制御ルールとして式（２）を受け取るので、ＰＲＯＣフィールドの指定「ＤＲＯＰ」に従い、当該ＳＹＮパケットを廃棄する（図１４参照）。

【００６５】

以上のような動作を行うことにより、本発明による攻撃防御システムは、攻撃元ホスト３０１上のワームからの攻撃から、内部ネットワーク４上のサーバ装置４０１を保護することができる。

【００６６】

（第２実施形態）

２．１）構成

図１５は、本発明の第２実施形態による攻撃防御システムのブロック図である。本実施形態のファイアウォール装置５は、図２に示す第１実施形態におけるファイアウォール装置１に信頼度管理部５０２を加え、さらに誘導部１０３に代えて、信頼度に依存してパケット誘導方向を決定できる誘導部５０１を有する。以下、図２に示すシステムと同じ機能ブロックについては、同一参照番号を付して詳細な説明は省略する。

【００６７】

図１５において、誘導部５０１は、パケットを入力すると、信頼度管理部５０２へ入力ＩＰパケットのソースＩＰアドレスを出力し、対応する信頼度を取得する。信頼度を受け取ると、誘導部５０１はその信頼度と所定のしきい値との比較を行い、その結果に応じて、当該入力ＩＰパケットを第1の内部通信インタフェース１０４および第２の内部通信インタフェース１０５のいずれかに出力する。

【００６８】

信頼度管理部５０２はＩＰアドレスと対応する信頼度との組の集合を管理する。誘導部５０１から要求があると、信頼度管理部５０２はそれに対応した信頼度を検索して誘導部５０１へ返し、後述するように信頼度の更新を行う。

【００６９】

２．２）動作

図１６は、本発明の第２実施形態による攻撃防御システムの動作を示すフローチャートである。

【００７０】

まず、第１実施形態のファイアウォール装置１と同様に、インターネット３からの入力ＩＰパケットを受信すると（ステップＡ１）、パケットフィルタ１０１は、アクセス制御リスト管理部１０２で保持されているアクセス制御ルールの内容に応じて、当該入力ＩＰパケットの受理または廃棄を行う（ステップＡ２）。受理されたＩＰパケットは誘導部５０１へ転送される。

【００７１】

２．２．１）信頼度管理

誘導部５０１は、入力ＩＰパケットに含まれる情報のうち少なくともソースＩＰアドレスを信頼度管理部５０２へ出力し、当該ＩＰアドレスに対する信頼度を取得する（ステップＣ１）。信頼度管理部５０２はＩＰアドレスとその信頼度との組の集合を保持し、ＩＰアドレスを入力すると、それに対応する信頼度を出力することができる。具体的には、例えば、「１．２．３．４：１０」などのように、「＜ＩＰアドレス＞：＜信頼度＞」といった形式をなす行で構成されるテキストファイルを用いることができる。

【００７２】

その他、検索および更新処理を効率的に行うために、リレーショナルデータベースを利用してもよい。いずれにせよ、任意のＩＰアドレスについて、対応する信頼度を適切に検索および更新できればよい。信頼度管理部５０２は、入力されたＩＰアドレスに対応するＩＰアドレスと信頼度との組が１つ見つかれば、当該信頼度を誘導部５０１へ出力する。もし適切なＩＰアドレスと信頼度の組が見つからなかった場合には、当該ＩＰアドレスに対する信頼度として初期値（例えば０）を設定し、当該初期値を誘導部５０１に出力するとともに、新たに「＜ＩＰアドレス＞：＜初期値＞」という組を保持内容に追加する。

【００７３】

続いて、信頼度管理部５０２は、信頼度を出力した後、当該信頼度を増加させるように保持内容を更新する（ステップＣ２）。具体的には、例えば次式（４）

に示されるように、信頼度に定数Ｃ（≧１）を加算する。

ｃ［ｎ＋１］＝ｃ［ｎ］＋Ｃ　　・・・　（４）。

【００７４】

２．２．２）信頼度に基づくパケット誘導

誘導部５０１は、取得した信頼度に応じて、当該ＩＰパケットの転送先を決定する（ステップＣ３）。信頼度ｃの評価処理の好適な一例としては、予め誘導部５０１にあるしきい値Ｔを設定しておき、信頼度ｃとしきい値Ｔとの比較結果（大小関係）を評価する。

【００７５】

図１７は、本実施形態における信頼度とパケット転送先の関係を示すグラフである。ここでは、ｃ≧Ｔのときには、入力ＩＰパケットを「信頼できる」と判定し、当該ＩＰパケットを内部通信インタフェース１０４を介して内部ネットワーク４へ伝達する。一方、ｃ＜Ｔのときには、内部通信インタフェース１０５を介して、おとり装置２へ伝達する。

【００７６】

なお、これ以降の動作は、図７に示す処理（ステップＡ４～Ａ８）と同じである。

【００７７】

２．２．３）信頼度の更新方法

図１６のステップＣ２における信頼度の更新方法は、上述した式（４）の他に、別の方法もある。次式（５）に示すように、誘導部５０１からの入力の一部に、入力ＩＰパケットｐのバイト数Ｌ（ｐ）を含めておき、その逆数１／Ｌ（ｐ）を加算するようにしても良い。

ｃ［ｎ＋１］＝ｃ［ｎ］＋１／Ｌ（ｐ）　　・・・　（５）。

【００７８】

この方法は、大きなサイズをもつＩＰパケットほど信頼度が増加しにくくなるように、重みづけを行うものである。一般に、バッファオーバーフロー攻撃やサービス妨害（ＤｏＳ）攻撃を目的としたＩＰパケットは正常な通信内容をもつＩＰパケットに比べて大きなサイズをもつことが多いため、こうした重みづけを施

すことで、これらの攻撃の可能性をもつ入力ＩＰパケットを、できるだけ長い期間、おとり装置２へ誘導することが可能になる。その結果、本発明による攻撃防御システムの防御性能を高めることができる。

【００７９】

また、別の一例として、誘導部５０１からの入力の一部に、入力ＩＰパケットのプロトコル番号を含めておき、予め設定されたプロトコル番号に一致した場合のみ、信頼度を更新する方法を併用してもよい。たとえば、予めプロトコル番号「６」を設定しておくことで、入力ＩＰパケットがＴＣＰである場合にのみ、信頼度を更新する。こうすることで、本格的な攻撃の前に準備的に行われるスキャン攻撃による、不要な信頼度の増加を抑える効果が得られる。もちろん、更新処理の条件として、プロトコル番号だけでなく、その他ＩＰヘッダ、ＴＣＰヘッダ、ＵＤＰヘッダなどに含まれる任意の情報を用いてもよいし、複数の条件を組み合わせた論理式を用いるようにしてもよい。

【００８０】

さらに別の一例として、入力ＩＰパケットについて、一般に外れ値検知として知られるような、統計的に「異常であること」の確からしさを求める方法を用いてもよい。具体的には、図１８に示すように、ＩＰアドレスと信頼度との組の集合に代えて、特開２００１－１０１１５４公報（本出願人による特許出願）に記載の外れ値度計算装置を信頼度管理部５０２に組み込む。この場合、誘導部５０１からは実数値や属性を表す離散値などを含む多次元のベクトル、たとえば、ｘ＝（入力ＩＰパケットの到達時刻、入力ＩＰパケットのサイズ、プロトコル番号）を入力する。

【００８１】

このような多次元ベクトルを入力した外れ値度計算装置は、それまでの入力から生成した確率密度分布などを基に、１個の実数値として表される「スコア値」を算出する。このスコア値は「異常であること」の確からしさを表しており、その値が大きいほど攻撃である可能性が高い、言い換えれば信頼度が低い。したがって、スコア値の逆数でもって、入力ＩＰパケットに対する信頼度とすることができる。

【００８２】

図１８（Ａ）は、外れ値度計算を用いた信頼度管理部５０２の概略的構成図であり、（Ｂ）は、その一例を示す詳細なブロック図である。この外れ値度計算を用いる方法は、上述したような「決定的な」信頼度の評価方法では捉えきれない（すなわち予期されない）攻撃を「確率的に」検出するものである。したがって、将来現れうる未知の攻撃に対する防御が可能となる。

【００８３】

本発明の第２実施形態は、第１実施形態による効果に加えて、さらに「アクティブ・ターゲッティング」にも対応できるという効果が得られる。アクティブ・ターゲッティングとは、次に具体的に説明するように、予め特定のサーバ装置もしくはホスト装置に狙いを定めて行われる攻撃形態を指し、一般的には悪意をもった人間によって実行される。

【００８４】

２．３）具体例

図１９～図２１は、本実施形態による攻撃防御システムの具体的な動作を説明するためのネットワーク構成図である。

【００８５】

図１９に示すように、インターネット３上の攻撃元ホスト３０１を使うユーザが、内部ネットワーク４上のサーバ装置４０１の動作停止を目的として、Ｐｉｎｇ　Ｏｆ　ＤｅａｔｈなどのＤｏＳ攻撃を行う場合を考える。

【００８６】

このような場合、攻撃元ホスト３０１のＩＰアドレス「１２．３４．５６．７８」に対する信頼度が、誘導部５０１に設定されたしきい値以下であれば、図２０に示すように、ＤｏＳ攻撃を構成するＩＰパケットはおとり装置２へ誘導され、サーバ装置４０１は保護される。ＤｏＳ攻撃をしかけるような悪意をもった人間は、ターゲットを定めたしばらく後に、攻撃を開始すると考えられるので、前記しきい値を十分大きく設定しておくことで、おとり装置２によるサーバ装置４０１の保護が達成される。

【００８７】

さらに、通常の（すなわち攻撃の意図がない）ユーザからのアクセスについては、安全に内部ネットワーク４上のサーバ装置４０１によるサービスを行うができる。たとえば、図２１に示すように、インターネット３上に通常のホスト３０２から、サーバ装置４０１へのアクセスがあった場合、前記例と同様に、ファイアウォール装置５の信頼度管理部５０２により、通常のホスト３０２のＩＰアドレスに対する信頼度が評価される。

【００８８】

もし、通常のホスト３０２の信頼度が不十分であれば、誘導部５０１により「不審」と判定され、おとり装置２へ当該アクセスを構成するＩＰパケットは誘導される。ここで、おとり装置２のプロセッサ２０１で、サーバ装置４０１上のWWWサービスと同じ処理を行うよう、おとり装置２を設定しておく。すなわち、おとり装置２をサーバ装置４０１のミラーサーバとして動作させる。具体的には、WWWサービスの場合、HTMLファイルやJPEGファイルなどのコンテンツの複製をとればよい。したがって、通常のホスト３０２は目的のサービスを受けることができる。おとり装置２では正常なアクセスがなされる間は攻撃が検知されることがないので、通常のホスト３０２のＩＰアドレスに対する信頼度は上述した信頼度更新方法に従って増加していき、いずれ、しきい値Ｔを超える。信頼度ｃがしきい値Ｔを超えた後は、通常のホスト３０２からのアクセスを構成するＩＰパケットは内部ネットワーク４内のサーバ装置４０１へ誘導される。

【００８９】

このような動作により、信頼ずみの通常のユーザからのアクセスについては、すべてサーバ装置４０１が応答する。したがって、おとり装置２が攻撃を受けて、その動作を停止したとしても、信頼ずみの通常のユーザは、サーバ装置４０１によりサービスを継続して受けることができるという効果をもつ。

【００９０】

なお、おとり装置２はサーバ装置４０１上の完全なミラーサーバとして設定してもよいし、例えば、ユーザ認証を要するような重要サービスは除いて、一般的なサービスだけをおとり装置２で提供するようにも設定できる。

【００９１】

（第３実施形態）

図２２は、本発明の第３実施形態による攻撃防御システムのファイアウォール装置の概略的構成を示すブロック図であり、図２３は、その一例を示す詳細なブロック図である。本実施形態のファイアウォール装置６は、ファイアウォール装置１における誘導部１０３に加えて、図５に示す第２実施形態の誘導部５０１および信頼度管理部５０２を有する。

【００９２】

具体的には、図２３に示すように、第１の誘導部１０３の後段として第２の誘導部５０１を設けても良い。逆に、第１の誘導部１０３の前段として第２の誘導部５０１を設けることもできる。

【００９３】

いずれの構成においても、ワームのようにランダムにＩＰアドレスを選択して行われる攻撃と、アクティブ・ターゲッティングによる攻撃の両方に対応できる、という効果が得られる。また、あるホストが、第２の誘導部５０１で一旦信頼された後、ワームに感染するなどした場合でも、おとり装置２にて攻撃の有無を検査することができる、という効果も得られる。

【００９４】

（第４実施形態）

４．１）構成

図２４は、本発明における第４実施形態による攻撃防御システムのファイアウォール装置の一例を示すブロック図である。本実施形態よるファイアウォール装置７は、図１５のファイアウォール装置５における信頼度管理部５０２に代えて、信頼度管理部７０１が接続されている。その他の機能ブロックは、図１５のものと同じであるから、同一参照番号を付して説明は省略する。

【００９５】

図２４に示すように、信頼度管理部７０１は、リアルタイム信頼度データベース７０１１、複製処理部７０１２、長期信頼度データベース７０１３、および、更新処理部７０１４を備える。

【００９６】

リアルタイム信頼度データベース７０１１は、ＩＰアドレス、それに対応する信頼度および最終更新時刻の組の集合を管理し、誘導部５０１からの問い合わせのＩＰアドレスに応じて、対応する信頼度を返す。複製処理部７０１２は、定期的に、リアルタイム信頼度データベース７０１１の内容を、長期信頼度データベース７０１３へ複製する。

【００９７】

長期信頼度データベース７０１３は、ＩＰアドレス、それに対応する信頼度および最終更新時刻の組の集合を管理する。更新処理部７０１４は、定期的に長期信頼度データベース７０１３を参照し、所定の期間よりも古い最終更新時刻を有する項目について、その信頼度を減算する更新処理を実行する。

【００９８】

４．２）信頼度管理

基本的には、入力ＩＰパケットをフィルタリングし、おとり装置２または内部ネットワーク３へ誘導するまでの処理は、第２実施形態のファイアウォール装置５と同一である（図１６のステップＡ１～Ａ２、Ｃ１～Ｃ３、Ａ４～Ａ８）。ただし、本実施形態の信頼度管理部７０１は、パケットの処理と並行して、以下にあげるような信頼度管理処理を行う。

【００９９】

図２５は信頼度管理部７０１における信頼度参照処理を示すフローチャートである。まず、図１６のステップＣ１において信頼度の参照が行われたとき、信頼度管理部７０１は、リアルタイム信頼度データベース７０１１から、入力として与えられたＩＰアドレスに対応する項目が記録されているかどうかを調べる（図２５のステップＤ１）。当該ＩＰアドレスに対応する項目が記録されている場合（ステップＤ１のＹ）、さらにその信頼度を参照し、当該信頼度を誘導部５０１に出力する（ステップＤ２）。

【０１００】

一方、ＩＰアドレスに対応する項目がリアルタイム信頼度データベース７０１１に記録されていない場合（ステップＤ１のＮ）、まず、長期信頼度データベース７０１３を参照して、当該ＩＰアドレスに対応する項目が記録されているかど

うかを調べる（ステップＤ３）。記録されている場合（ステップＤ３のＹ）、長期信頼度データベース７０１３の該当項目の内容（ＩＰアドレス、信頼度および最終更新時刻）を、リアルイム信頼度データベース７０１１にコピーし（ステップＤ４）、信頼度を出力する（ステップＤ２）。長期信頼度データベース７０１３にも該当項目がない場合（ステップＤ３のＮ）、リアルタイム信頼度データベース７０１１に、所定の信頼度の初期値をもって、新たな項目を追加し（ステップＤ５）、信頼度を出力する（ステップＤ２）。

【０１０１】

そして、図１６のステップＣ２において信頼度の更新が行われたとき、信頼度管理部７０１は、ＩＰアドレスと、信頼度の更新に加えて、更新時刻をリアルタイム信頼度データベース７０１１に記録する。

【０１０２】

４．３）リアルタイム信頼度の複製処理

以上の処理に並行して、複製処理部７０１２は定期的に（例えば1日ごとに）リアルタイム信頼度データベース７０１１の全内容を走査しながら、各項目を長期信頼度データベース７０１３へコピーしていく。このとき、最終更新時刻を参照して、所定の期間（例えば1週間）以上、更新処理が行われなかった項目について、当該項目をリアルタイム信頼度データベース７０１１から削除する処理を行っても良い。

【０１０３】

４．４）長期信頼度の更新処理

また、更新処理部７０１４は、定期的に（例えば１日ごとに）長期信頼度データベース７０１３の全内容を走査しながら、各項目の最終更新時刻を参照して、所定の期間（例えば１週間）以上、更新が行われなかった項目については、その信頼度を所定の値だけ減算する。もしくは、単に削除しても良い。

【０１０４】

４．５）効果

以上のような動作を行うことで、リアルタイム信頼度データベース７０１１の記憶容量を抑えることができるので、ＳＤＲＡＭなど、低容量で高速な記憶デバ

イスを用いることができる。一方、長期信頼度データベース７０１３はアクセス頻度が少ないので、ハードディスクデバイスなど、大容量で低速な記憶デバイスを用いることができる。

【０１０５】

また、更新処理部７０１４による長期信頼度データベース７０１３の更新処理により、たとえ１度、十分な信頼度を得たソースＩＰアドレスについても、ある一定期間以上、アクセスが途絶えた場合には再び「不審」と見なすことができる。これは、特に中古ＰＣの売買など、ソースＩＰアドレスに相当するホストの利用環境が大きく変化した場合などに、信頼度の再評価を自動的におこなうことができるという効果をもつ。

【０１０６】

（第５実施形態）

本発明の第５実施形態として、図２３に示す第３実施形態の信頼度管理部５０２に代えて、上述した第４実施形態の信頼度管理部７０１を用いたファイアウォール装置を構成することができる。基本的な構成は図２３と同じであり、信頼度管理部７０１の構成及び動作は、図２４、図２５および第４実施形態の項で説明した通りであるから、ここでは省略する。

【０１０７】

（第６実施形態）

６．１）構成

図２６は、本発明の第６実施形態による攻撃防御システムのファイアウォール装置９を示す概略的ブロック図である。ファイアウォール装置９では、第１実施形態のファイアウォール装置１における誘導部１０３に代えて、バッファ９０１１およびＩＣＭＰ監視部９０１２を有する誘導部９０１が設けられている。本実施形態では、第１実施形態のように誘導リストを設けることなく、ＩＣＭＰパケットを利用して同様の機能を実現できる。なお、簡略化のために、図２６では他の機能ブロックの表示が省略されている。

【０１０８】

バッファ９０１１は、次に述べるように、パケットフィルタ１０１より受け取

ったパケットを一時的に蓄積し、第１内部通信インタフェース１０５を介して内部ネットワークへ転送すると共に、ＩＣＭＰ監視部９０１２からの求めに応じて、蓄積したパケットを第２の内部通信インタフェース１０５を介しておとり装置２へ再送信する。ＩＣＭＰ監視部９０１２は、第１の内部通信インタフェース１０４におけるＩＣＭＰパケットの受信を監視し、特定のＩＣＭＰエラーパケットを検出したとき、バッファ９０１１に適切なパケット再送を要求する。以下、本実施形態の動作を詳述する。

【０１０９】

６．２）動作

図２７は本実施形態によるファイアウォール装置９の動作を示すフローチャートである。まず、第１実施形態のファイアウォール装置１と同様に、外部通信インタフェース１００を介してインターネット４から受信した入力ＩＰパケットについて、パケットフィルタ１０１によるフィルタリングを行う（ステップＡ１，Ａ２）。

【０１１０】

受理されたＩＰパケットは誘導部９０１のバッファ９０１１に蓄積され（ステップＥ１）、無条件に第１の内部通信インタフェース１０４を介して内部ネットワーク３へ送出され（ステップＥ２）、通常のサービスが提供される（ステップＡ４）。この場合、たとえ不審パケットであっても内部ネットワークへ転送されてしまうが、実際の攻撃を実行する前に送信されるＴＣＰコネクション確立要求のＳＹＮパケットは攻撃要素が含まれていないために、ＳＹＮパケットであれば受け入れても問題はない。内部ネットワークにＳＹＮパケットが転送され宛先が存在しなければ、到達不能を知らせるＩＣＭＰパケット（タイプ３）が返される。

【０１１１】

ＩＣＭＰ監視部９０１２は、第１の内部通信インタフェース１０４でＩＣＭＰパケット（ＲＦＣ７９２記載）が受信されると、当該ＩＣＭＰパケットの内容を参照して、到達不能を知らせるエラー（すなわちＩＣＭＰタイプ３）であるか否かを調べる（ステップＥ３）。到達不能を知らせるエラーであれば（ステップＥ

３のＹ）、そのＩＰヘッダ部をさらに参照し、少なくともソースＩＰアドレスもしくはディスティネーションＩＰアドレスを用いてバッファ９０１１に再送要求を行う（ステップＥ３）。その他のメッセージであった場合は、何もせず、監視を続ける。

【０１１２】

再送要求を受けたバッファ９０１１は、少なくともソースＩＰアドレスもしくはディスティネーションＩＰアドレスに従って、蓄積されたパケットから該当するパケットを抽出し、当該パケットを第２の内部通信インタフェース１０５を介して、おとり装置２へ再送する（ステップＥ４）。以下、すでに述べたステップＡ５～Ａ８が実行される。

【０１１３】

このように攻撃要素を含まないコネクション確立のためのパケットを利用することで、内部ネットワーク３の未使用ＩＰアドレスを誘導リストとして事前に設定することなしに、自動的に未使用ＩＰアドレス宛ての入力ＩＰパケットをおとり装置２へ誘導することができる。

【０１１４】

（第７実施形態）

７．１）構成

図２８は、本発明の第７実施形態による攻撃防御システムのファイアウォール装置１０を示す概略的ブロック図である。このファイアウォール装置１０は、上述した第２～第５実施形態によるファイアウォール装置における防御ルール判定部１０７およびアクセス制御リスト管理部１０２に代えて、有効期限付き防御ルール判定部１００１および有効期限付きアクセス制御リスト管理部１００２を設けている。

【０１１５】

防御ルール判定部１００１は、制御インタフェース１０６を介しておとり装置２から受け取ったアラートに応じて、信頼度管理部５０２および７０１に対して、対応する信頼度の再設定を指示する。あるいは、アラートに応じて、更新すべきアクセス制御ルールを決定し、アクセス制御リスト管理部１００２にその更新

を指示する。

【０１１６】

信頼度管理部５０２および７０１は、防御ルール判定部１００１からの更新指示を受けて、新たな信頼度を決定し誘導部５０１へ出力する。アクセス制御リスト管理部１００２は、防御ルール判定部１００１からの更新指示を受けて、アクセス制御リストを更新し、パケットフィルタ１０１からの要求に応じてアクセス制御ルールを出力する。

【０１１７】

７．２）動作

本実施形態における攻撃防御システムの動作を、具体的な例を挙げながら詳細に説明する。

【０１１８】

まず、インターネット４から到達した入力ＩＰパケットが、ファイアウォール装置１０によって、おとり装置２へ誘導され、おとり装置２において、当該入力ＩＰパケットによる攻撃が検知され、その旨を知らせるアラートが送信されるまでは、図１６のステップＡ１～Ａ７に示すように、第２～第５実施形態における攻撃防御システムと同様である。

【０１１９】

ファイアウォール装置１０の防御ルール判定部１００１には、防御ルール判定部１０７とは異なり、信頼度を更新するための防御ルールが予め設定されている。例えば、防御ルールとして、次式（６）のような形式の記述があれば、信頼度を１減算すると解釈されるものとする。

ＲＥＣＯＮ：ｃ（＄｛ＳＯＵＲＣＥ＿ＩＰ＿ＡＤＤＲＥＳＳ｝）－＝１

・・・　（６）。

【０１２０】

たとえば、制御インタフェース１０６を通してソースＩＰアドレス「１２．３４．５６．７８」を示すアラートが受け取ると、防御ルール判定部１００１はＩＰアドレス「１２．３４．５６．７８」に対する信頼度を１減算すると解釈し、その旨を信頼度管理部５０２／７０１に指示する。すなわち、アラートを受け取

ると、そのソースＩＰアドレスの信頼度を低減させる。信頼度管理部５０２は第２実施形態で説明したように信頼度を更新し、信頼度管理部７０１は第４実施形態で説明したように信頼度を更新するから、信頼度の低減処理を加えることで、よりきめ細かい信頼度管理ができる。

【０１２１】

また、ファイアウォール装置１０において、防御ルール判定部１００１内に、防御ルール判定部１０７と同様に、アクセス制御ルールのひな型としての防御ルールを予め設定してもよい。ただし、この場合のアクセス制御ルールは、新たに「有効期間」を表すフィールドを記載できる（したがって防御ルールにも記載可能）。例えば、次式（７）に示すように、前記式（１）の防御ルールにＥＸＰＩＲＥの項を追加し、「７日間有効」という制約をつけることができる。

ＩＮＴＲＵＳＩＯＮ：（ＳＲＣ：＄｛ＳＯＵＲＣＥ＿ＩＰ＿ＡＤＤＲＥＳＳ｝，ＤＳＴ：＊，ＰＲＯＣ：ＤＲＯＰ，ＥＸＰＩＲＥ：＋７ＤＡＹ）　・・・（７）

。

【０１２２】

したがって、アラートが制御インタフェース１０６を経由して防御ルール判定部１００１に伝達されると、防御ルール判定部１０７と同様の方法で、次式（８）に示すようにアクセス制御ルールが生成され、アクセス制御リスト管理部１００２に伝達される。

（ＳＲＣ：１２．３４．５６．７８，ＤＳＴ：＊，ＰＲＯＣ：ＤＲＯＰ，ＥＸＰＩＲＥ：＋７ＤＡＹ）　・・・　（８）。

【０１２３】

次に、アクセス制御リスト管理部１００２は、防御ルール判定部１００１から受け取ったアクセス制御ルールをアクセス制御リストデータベース１０２１に追加する。このとき、式（８）のようにＥＸＰＩＲＥフィールドがアクセス制御ルールに記載されている場合、アクセス制御リスト管理部１００２は、現在時刻に、ＥＸＰＩＲＥフィールドに指定された値を加算した時刻を算出した上で、データベースを更新する（図７のステップＡ８に対応する）。

【０１２４】

図２９は、アクセス制御リスト管理部１００２の管理動作を示すフローチャートである。アクセス制御リストデータベース１０２１が更新された後、再びソースアドレス「１２．３４．５６．７８」からの入力ＩＰパケットがファイアウォール装置１０に到達すると、パケットフィルタ１０１は当該ソースＩＰアドレスをアクセス制御リスト管理部１００２へ送付してアクセス制御ルールの取得要求を行う（ステップＡ２＿１）。

【０１２５】

アクセス制御リスト管理部１００２は、当該ソースＩＰアドレスに対応するアクセス制御ルールを検索する（ステップＡ２＿２、Ａ２＿３）。式（８）に相当するアクセス制御ルールを抽出すると、アクセス制御リスト管理部１００２は、ＥＸＰＩＲＥフィールドに記載された有効期間と現在時刻とを比較する（ステップＡ２＿４）。

【０１２６】

現在時刻が有効期間を超過していた場合には（ステップＡ２＿４のＹＥＳ）、当該アクセス制御ルールをアクセス制御リストデータベース１０２１から削除し（ステップＡ２＿５）、デフォルトのアクセス制御ルールをパケットフィルタ１０１へ返す（ステップＡ２＿６）。逆に、有効期間内であれば（ステップＡ２＿４のＮＯ）、次式（９）に示すようなＥＸＰＩＲＥフィールドを除いたアクセス制御ルールをパケットフィルタ１０１へ返す（ステップＡ２＿７）。

（ＳＲＣ：１２．３４．５６．７８，ＤＳＴ：＊，ＰＲＯＣ：ＤＲＯＰ）

・・・（９）。

【０１２７】

こうして取得したアクセス制御ルールを用いて、パケットフィルタ１０１は受信ＩＰパケットの受理／廃棄の判定を行う（ステップＡ２）。

【０１２８】

上述したように、攻撃をおとり装置で検知した後の防御方法として、よりきめ細かな対策を講じることができる。具体例を挙げると、一般に攻撃者は、「侵入」もしくは「破壊」に相当する攻撃の準備として、ポートスキャンあるいはＴｒａｃｅｒｏｕｔｅなどの「探査」に相当する攻撃を行う。しかし、「探査」とし

て検出されるアクセスが、全て攻撃であるとは限らないことも、よく知られる所である。したがって、「探査」に対する防御方法として、恒久的なアクセス遮断を行うことは不都合を生じる可能性がある。

【０１２９】

そこで、本実施形態では、有効期限付きのアクセス制御ルールを用いて時間制限を付けたアクセス遮断を行う。または、上述したように、アラーム発生によってそれまで蓄積された信頼度を低減させることで、信頼度がしきい値Ｔ（図１７参照）を超えないようにし、おとり装置への誘導を継続し、後で「侵入」もしくは「破壊」に相当する攻撃を検知してから恒久的なアクセス遮断へと対応を変えることもできる。

【０１３０】

（第８実施形態）

図３０は、本発明の第８実施形態による攻撃防御システムの概略的構成図である。第８実施形態では、単一のおとり装置２に代えて、２台以上のおとり装置２を含むおとりクラスタ２１が設けられている。

【０１３１】

本実施形態における各おとり装置２は、特定のディスティネーションＩＰアドレスをもつパケット、もしくは、特定のポート番号をもつパケットにしか偽のサービスを提供しないようにする。

【０１３２】

こうすることにより、内部ネットワーク４上の特定のサーバ装置に１対１対応するおとり装置２を設けたり、特定の偽のサービスだけを提供するおとり装置２を設けたりすることができる。したがって、攻撃者に対して正規のサーバ装置により近いサービスを提供することができ、また、特定のサービス向けの正常動作定義をもつことでより運用性を向上させることもできる。

【０１３３】

（第９実施形態）

第９実施形態のファイアウォール装置は、第１～第８実施形態における誘導部に加えて、出力パケット誘導部を有する。出力パケット誘導部は、内部ネットワ

ーク３からインターネット４へ向けて送信される出力ＩＰパケットに対して、上述したパケットフィルタリングおよびおとり装置への誘導処理を行う。

【０１３４】

このような出力パケット誘導部を設けることで、内部ネットワーク３の運用規定として、インターネット４へのアクセスを禁じているような場合に、内部ネットワーク３からインターネット４への不法なアクセスを検知し、その記録をとることができる。

【０１３５】

（第１０実施形態）

上記第１～第９実施形態の説明では機能ブロック構成を用いたが、本発明はこれに限定されるものではなく、ソフトウエアにより同一の機能を実現することもできる。

【０１３６】

図３１は、本発明の第１０実施形態による攻撃防御システムの概略的構成図である。本実施形態のファイアウォール装置には、プログラム制御プロセッサ１１０１、上記第１～第９実施形態におけるそれぞれの機能ブロックを実現するプログラムのセットを格納したプログラムメモリ１１０２、アクセス制御リストデータベースや防御ルール判定用のデータベースなどを格納したデータベース１１０３、および各種インタフェース１００、１０４～１０６が設けられている。同様に、本実施形態のおとり装置には、プログラム制御プロセッサ２１０１、上記第１実施形態で説明したおとり装置としての機能ブロックを実現するプログラムのセットを格納したプログラムメモリ２１０２およびファイアウォール装置とのインタフェースが設けられている。本実施形態の動作は、プログラムメモリに格納されるプログラムセットを上記第１～第９実施形態のいずれかに設定することで、所望の実施形態による攻撃防御システムを実現することができる。

【０１３７】

（第１１実施形態）

上記第１～第１０実施形態では、ファイアウォール装置とおとり装置とが別ユニットになった攻撃防御システムを例示したが、本発明はこれに限定されるもの

ではなく、ハードウエア的に１ユニットで構成することもできる。１ユニットは、取り扱いが容易であり小型化し易いというメリットがある。

【０１３８】

図３２は、本発明の第１１実施形態による攻撃防御ユニットの概略的構成図である。本実施形態の攻撃防御ユニットには、ファイアウォール装置用のプログラム制御プロセッサ１１０１、おとり装置用のプログラム制御プロセッサ２１０１、アクセス制御リストデータベースや防御ルール判定用のデータベースなどを格納したデータベース１１０３、上記第１～第９実施形態におけるそれぞれの機能ブロックを実現するプログラムのセットを格納したプログラムメモリ１１０４、および各種インタフェース１００および１０４が設けられている。本実施形態の動作は、プログラムメモリに格納されるプログラムセットを上記第１～第９実施形態のいずれかに設定することで、所望の実施形態による攻撃防御システムを実現することができる。また、プロセッサ１１０１とプロセッサ２１０１とを単一のプロセッサで構成しても良い。

【０１３９】

【発明の効果】

以上詳細に説明したように、本発明による攻撃防御システム及び方法によれば、ＩＰパケットのヘッダ情報に基づいてパケットの誘導を行うために、外部ネットワークから内部ネットワークへのアクセスにおいて通信路暗号化技術が用いられた場合でも、攻撃を検知および防御することができる。いかなる通信路暗号化技術が用いられたとしても、少なくともＩＰヘッダに記載されたソースＩＰアドレスもしくはディスティネーションＩＰアドレスは暗号化されず、さらにファイアウォール装置によるおとり装置への誘導は、これらＩＰヘッダに記載された情報を基に行うことができるためである。

【０１４０】

また、本発明によれば、ファイアウォール装置によるおとり装置への誘導方法が少ないパラメータを基にした簡易なアルゴリズムで実現できるため、高速ネットワーク環境においても、ネットワーク性能を高いレベルで維持できる。

【０１４１】

さらに、本発明によれば、おとり装置へ誘導されて攻撃が検出された全てのパケットについて、その送信元ホストからの以降のアクセスを拒否するように動的な防御を行うことで後続する攻撃を全てファイアウォール装置で防御することができる。このために内部ネットワークへの通信経路が無くなり、検出された攻撃用パケットが一切内部ネットワークに到達しない。

【図面の簡単な説明】

【図１】

本発明による攻撃防御システムの概略的ブロック図である。

【図２】

本発明の第１実施形態による攻撃防御システムのファイアウォール装置１およびおとり装置２の構成を示すブロック図である。

【図３】

図２のファイアウォール装置１におけるアクセス制御リスト管理部１０２の模式的構成図である。

【図４】

アクセス制御リストデータベース１０２１の内容を例示した模式図である。

【図５】

誘導部１０３に設けられた誘導リストの一例を示す模式図である。

【図６】

防御ルール判定部１０７に保持されているアクセス制御ルールのひな型を例示した模式図である。

【図７】

本発明の第１実施形態による攻撃防御システムの動作を示すフローチャートである。

【図８】

本発明の第１実施形態のファイアウォール装置でアドレス変換処理を行う際の好適な一例を示すブロック図である。

【図９】

第１実施形態の具体的動作例を説明するためのネットワーク構成図である。

【図１０】

第１実施形態の具体的動作例を説明するためのネットワーク構成図である。

【図１１】

第１実施形態の具体的動作例を説明するためのネットワーク構成図である。

【図１２】

おとり装置２における攻撃検知動作を説明するための模式図である。

【図１３】

第１実施形態におけるアクセス制御リストの更新動作例を説明するための模式図である。

【図１４】

第１実施形態の具体的動作例を説明するためのネットワーク構成図である。

【図１５】

本発明の第２実施形態による攻撃防御システムのブロック図である。

【図１６】

本発明の第２実施形態による攻撃防御システムの動作を示すフローチャートである。

【図１７】

本実施形態における信頼度とパケット転送先の関係を示すグラフである。

【図１８】

（Ａ）は、外れ値度計算を用いた信頼度管理部５０２の概略的構成図であり、（Ｂ）は、その一例を示す詳細なブロック図である。

【図１９】

本実施形態による攻撃防御システムの具体的な動作を説明するためのネットワーク構成図である。

【図２０】

本実施形態による攻撃防御システムの具体的な動作を説明するためのネットワーク構成図である。

【図２１】

本実施形態による攻撃防御システムの具体的な動作を説明するためのネットワ

ーク構成図である。

【図２２】

本発明の第３実施形態による攻撃防御システムのファイアウォール装置の概略的構成を示すブロック図である。

【図２３】

第３実施形態による攻撃防御システムのファイアウォール装置の一例を示す詳細なブロック図である。

【図２４】

本発明における第４実施形態による攻撃防御システムのファイアウォール装置の一例を示すブロック図である。

【図２５】

信頼度管理部７０１における信頼度参照処理を示すフローチャートである。

【図２６】

本発明の第６実施形態による攻撃防御システムのファイアウォール装置９を示す概略的ブロック図である。

【図２７】

本実施形態によるファイアウォール装置９の動作を示すフローチャートである。

【図２８】

本発明の第７実施形態による攻撃防御システムのファイアウォール装置１０を示す概略的ブロック図である。

【図２９】

アクセス制御リスト管理部１００２の管理動作を示すフローチャートである。

【図３０】

本発明の第８実施形態による攻撃防御システムの概略的構成図である。

【図３１】

本発明の第１０実施形態による攻撃防御システムの概略的構成図である。

【図３２】

本発明の第１１実施形態による攻撃防御ユニットの概略的構成図である。

【符号の説明】

１　ファイアウォール装置

１００　外部通信インタフェース

１０１　パケットフィルタ

１０２　第１のアクセス制御リスト管理部

１０２１　アクセス制御リストデータベース

１０２２　検索処理部

１０２３　更新処理部

１０３　誘導部

１０３１　アドレス変換部

１０４　第１の内部通信インタフェース

１０５　第２の内部通信インタフェース

１０６　制御インタフェース

１０７　防御ルール判定部

２　おとり装置

２０１　プロセッサ

２０２　攻撃検知部

３　インターネット

３０１　攻撃元ホスト

３０２　通常のホスト

４　内部ネットワーク

４０１　サーバ装置

５　ファイアウォール装置

５０１　誘導部

５０２　信頼度管理部

５０２１　外れ値検知部

６　ファイアウォール装置

７　ファイアウォール装置

７０１　信頼度管理部

７０１１　リアルタイム信頼度データベース

７０１２　複製処理部

７０１３　長期信頼度データベース

７０１４　更新処理部

８　ファイアウォール装置

９　ファイアウォール装置

９０１　誘導部

９０１１　バッファ

９０１２　ＩＣＭＰ監視部

１０　ファイアウォール装置

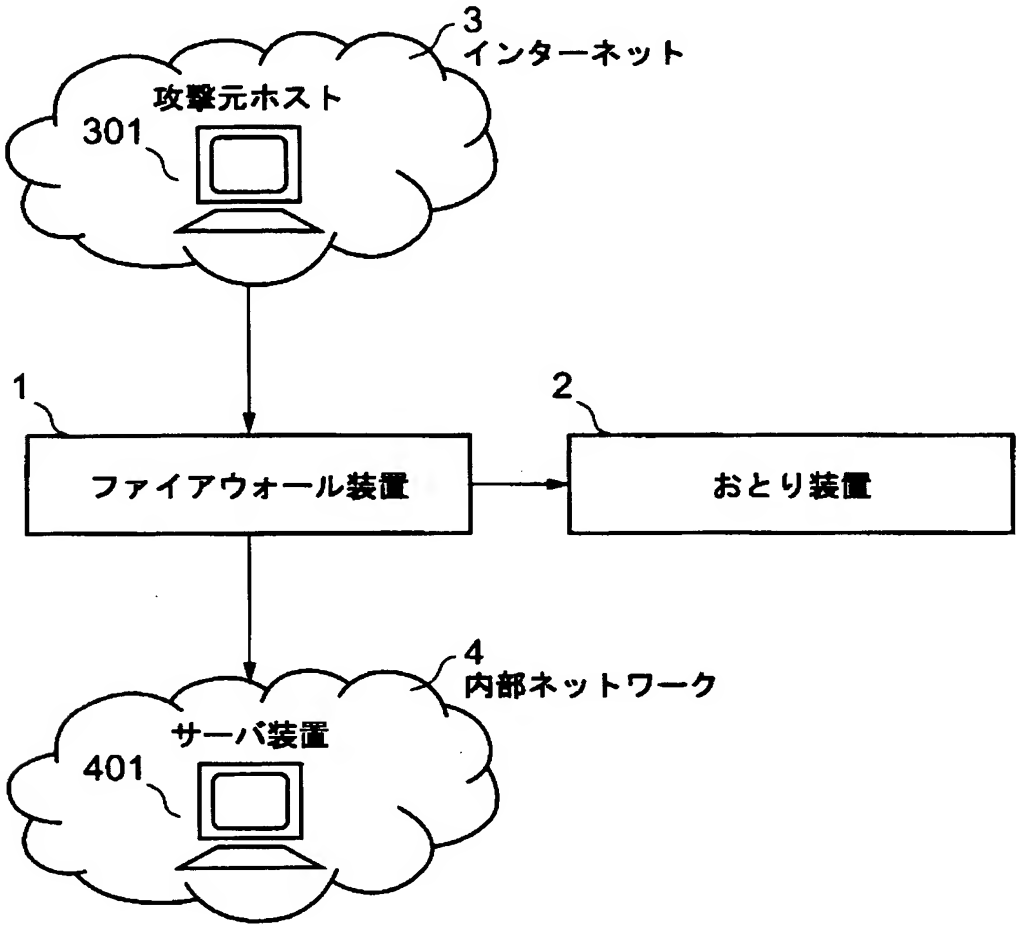
１００１　防御ルール判定部

１００２　アクセス制御リスト管理部

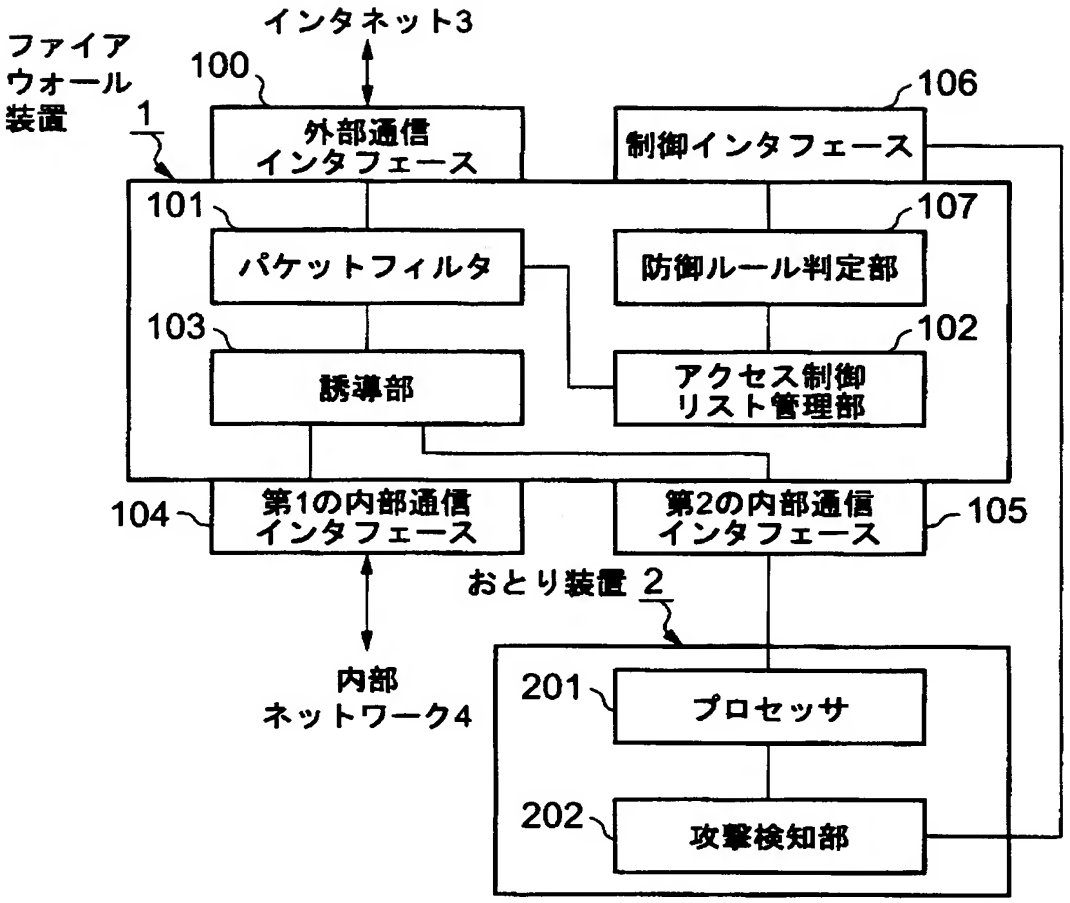
２１　おとりクラスタ

【書類名】　図面

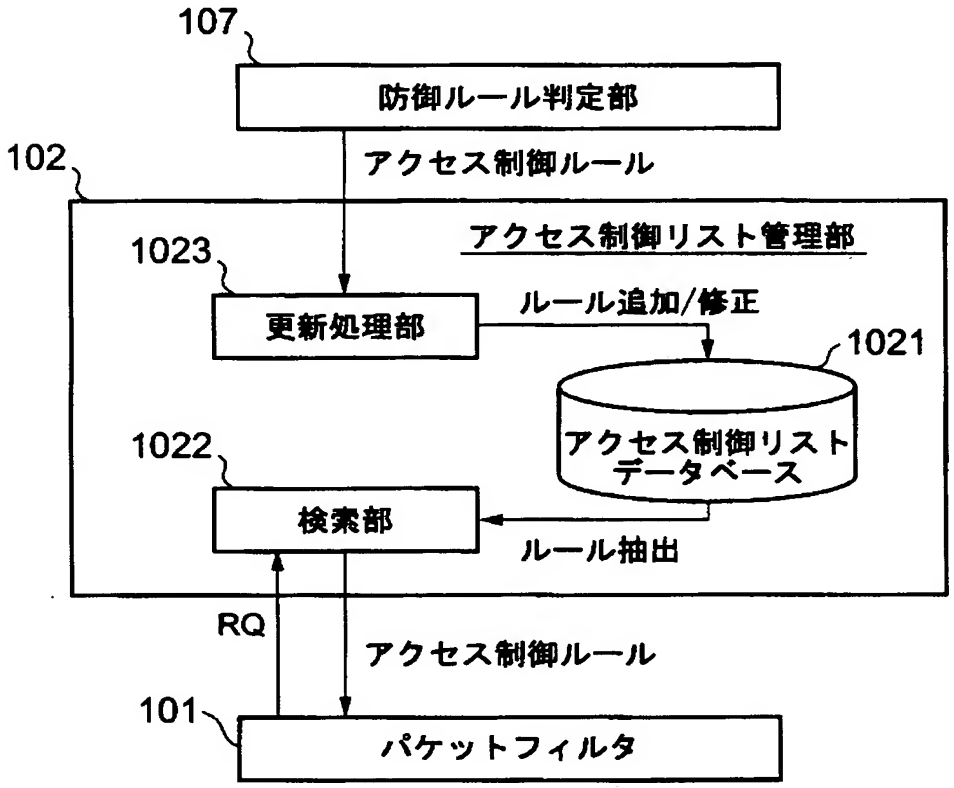
【図１】


3
インターネット
攻撃元ホスト
301
1
2
ファイアウォール装置
おとり装置
4
内部ネットワーク
サーバ装置
401

【図２】


インタネット3
ファイア
ウォール
装置
1
100
外部通信
インタフェース
106
制御インタフェース
101
パケットフィルタ
107
防御ルール判定部
103
誘導部
102
アクセス制御
リスト管理部
104
第1の内部通信
インタフェース
第2の内部通信
インタフェース
105
おとり装置 2
内部
ネットワーク4
201
プロセッサ
202
攻撃検知部

【図３】


107
防御ルール判定部
アクセス制御ルール
102
アクセス制御リスト管理部
1023
更新処理部
ルール追加/修正
1021
アクセス制御リスト
データベース
1022
検索部
ルール抽出
RQ
アクセス制御ルール
101
パケットフィルタ

【図４】

1021

アクセス制御リストデータベース

ソースIPアドレス (SRC)	ディスティネーション IPアドレス(DST)	パケットフィルタ処理 (PROC)
*	1.2.3.1	ACCEPT
*	1.2.3.2	ACCEPT
12.34.1.1	*	ACCEPT
*	1.2.3.3	DROP
*	*	DENY

*…任意のアドレスにマッチ
ACCEPT…パケットの受理
DENY…パケットの拒否(ICMPエラーを通知)
DROP…パケットの廃棄(ICMPエラーを通知しない)

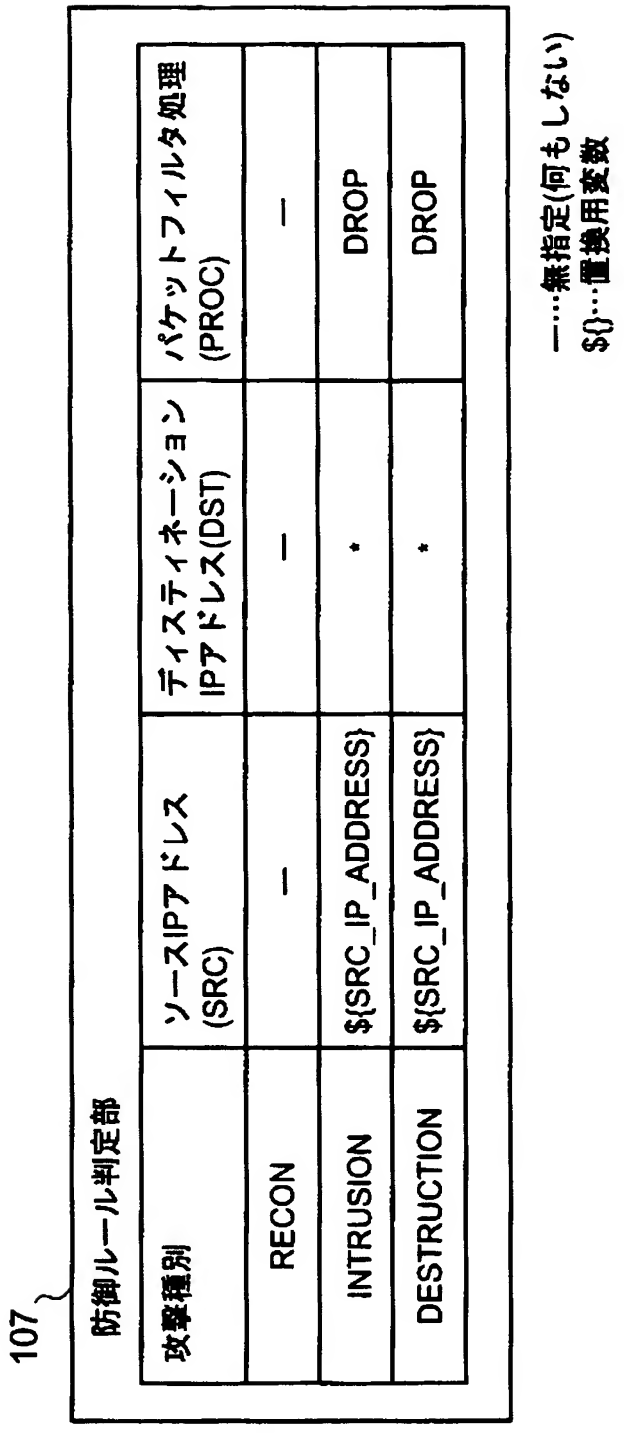
【図５】

誘導リスト

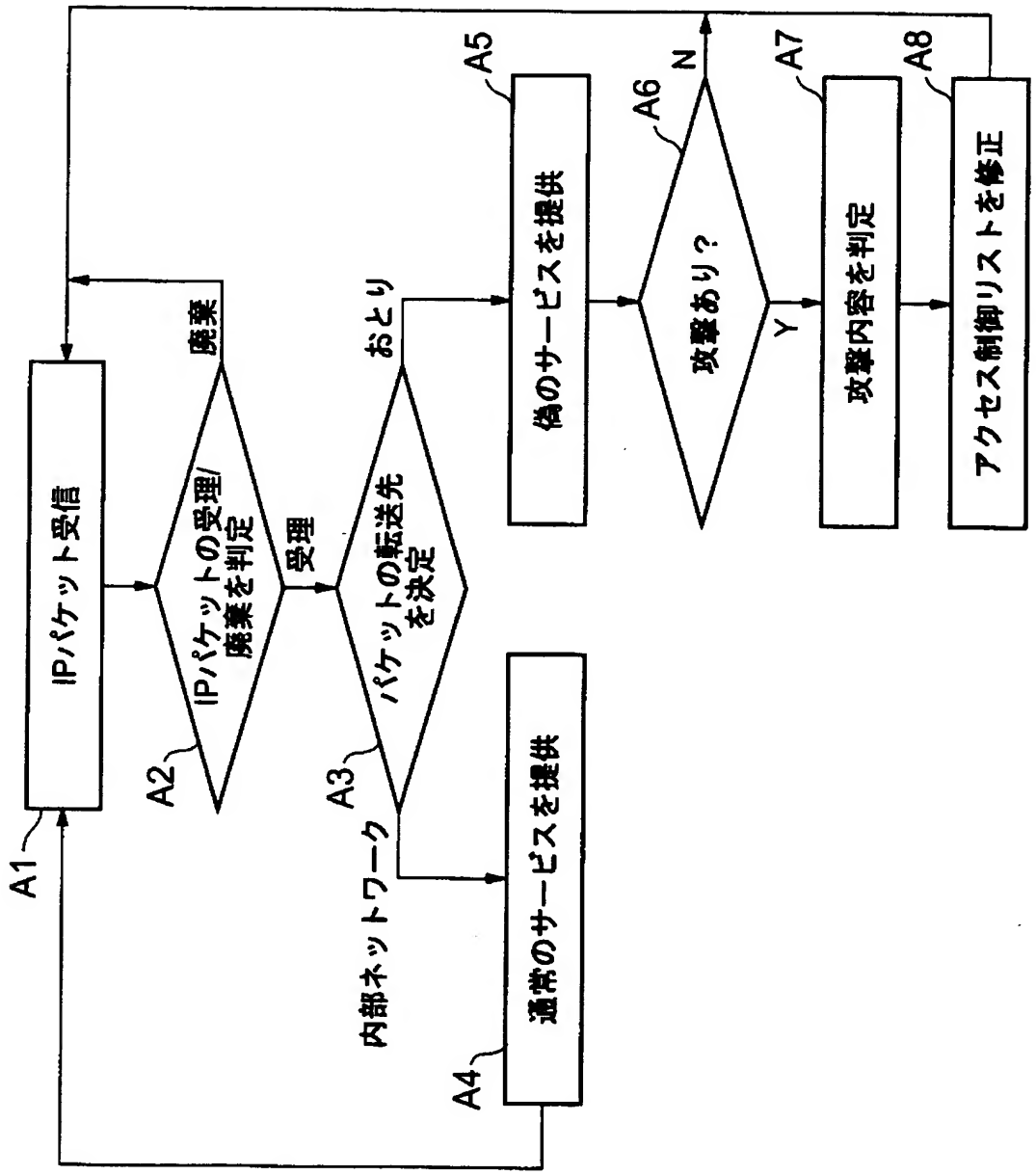
1. 2. 3. 1
1. 2. 3. 2
1. 2. 3. 3

1. 2. 3. 5
1. 2. 3. 6
⋮

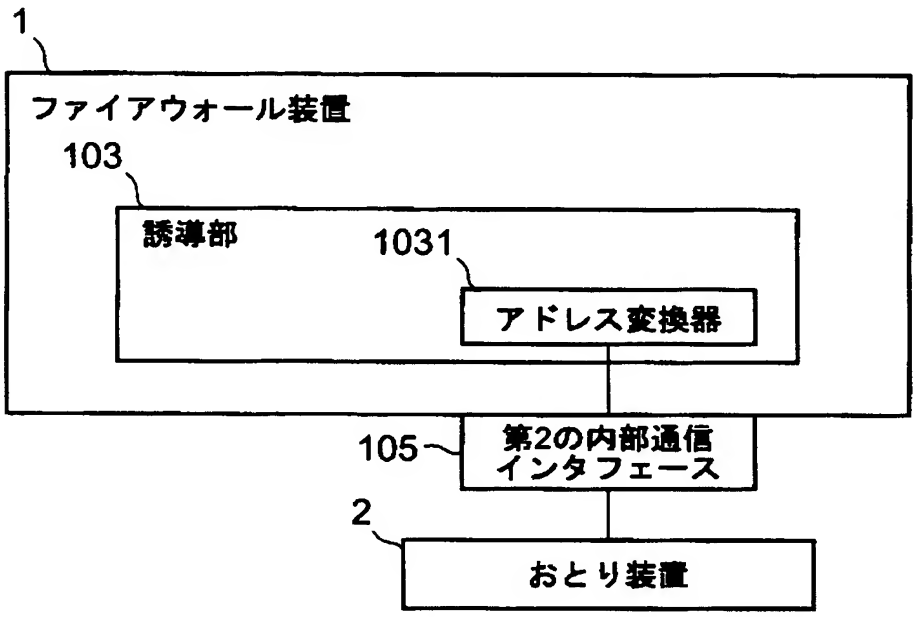
【図６】


107
防御ルール判定部
攻撃種別
ソースIPアドレス (SRC)
ディスティネーション IPアドレス(DST)
パケットフィルタ処理 (PROC)
RECON
—
—
—
INTRUSION
${SRC_IP_ADDRESS}
*
DROP
DESTRUCTION
${SRC_IP_ADDRESS}
*
DROP
—…無指定(何もしない)
${}…置換用変数

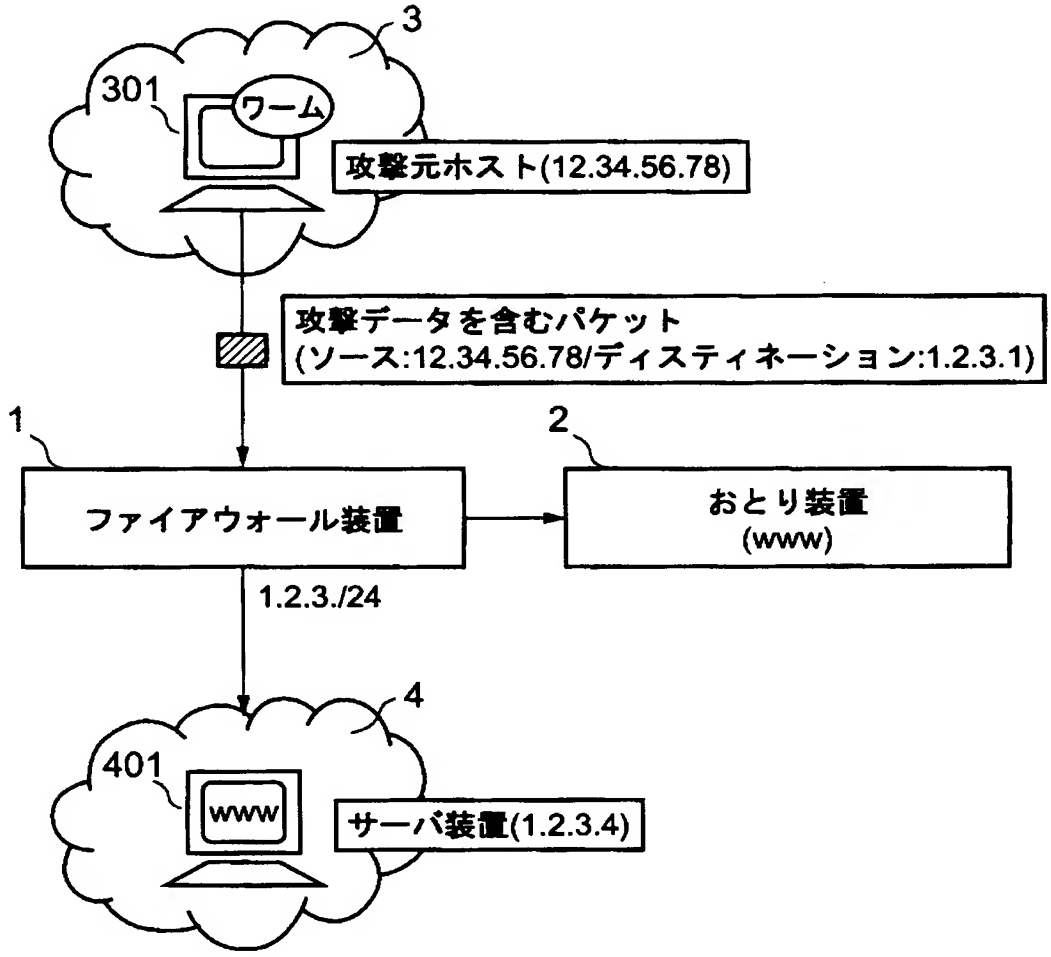
【図７】


IPパケット受信
A1
IPパケットの受理/
廃棄を判定
A2
廃棄
受理
パケットの転送先
を決定
A3
おとり
内部ネットワーク
通常のサービスを提供
A4
偽のサービスを提供
A5
攻撃あり？
A6
N
Y
攻撃内容を判定
A7
アクセス制御リストを修正
A8

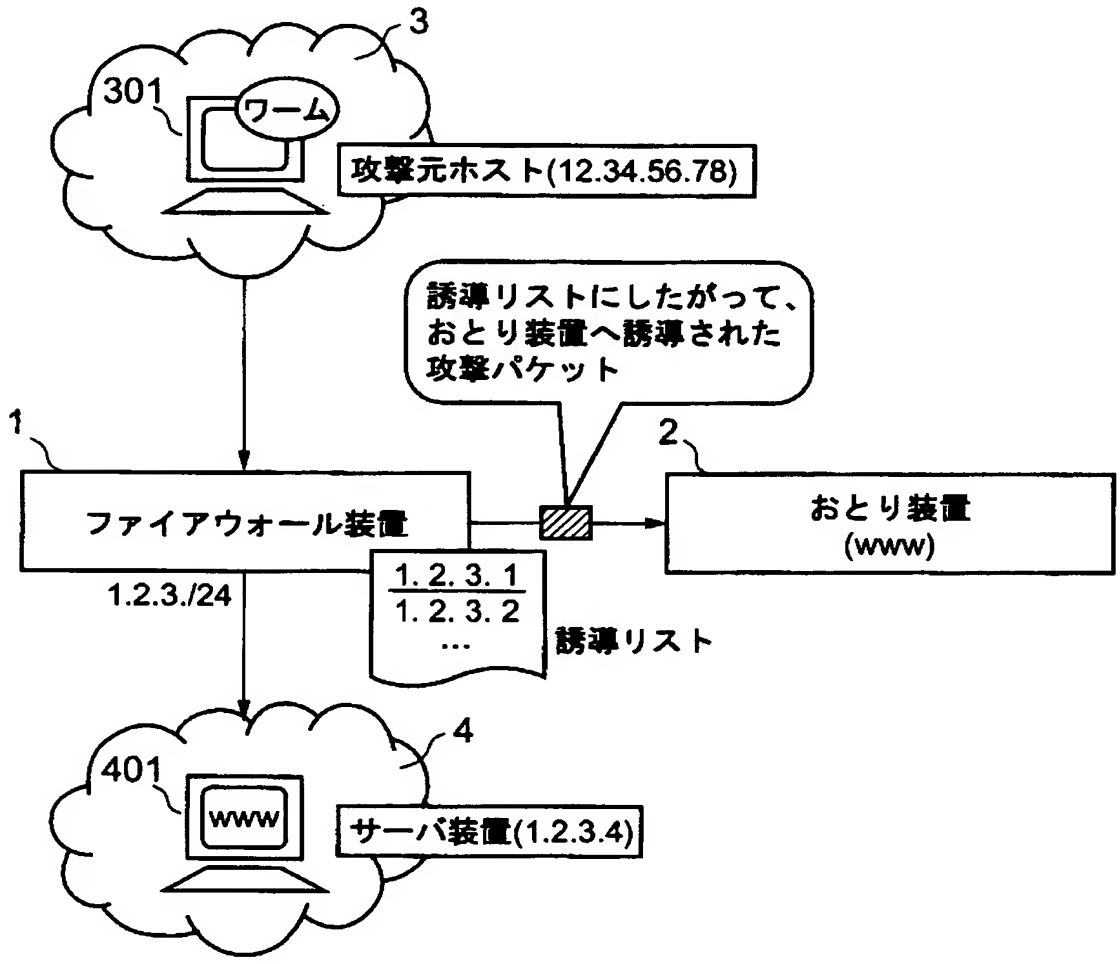
【図８】


1
ファイアウォール装置
103
誘導部
1031
アドレス変換器
105
第2の内部通信
インタフェース
2
おとり装置

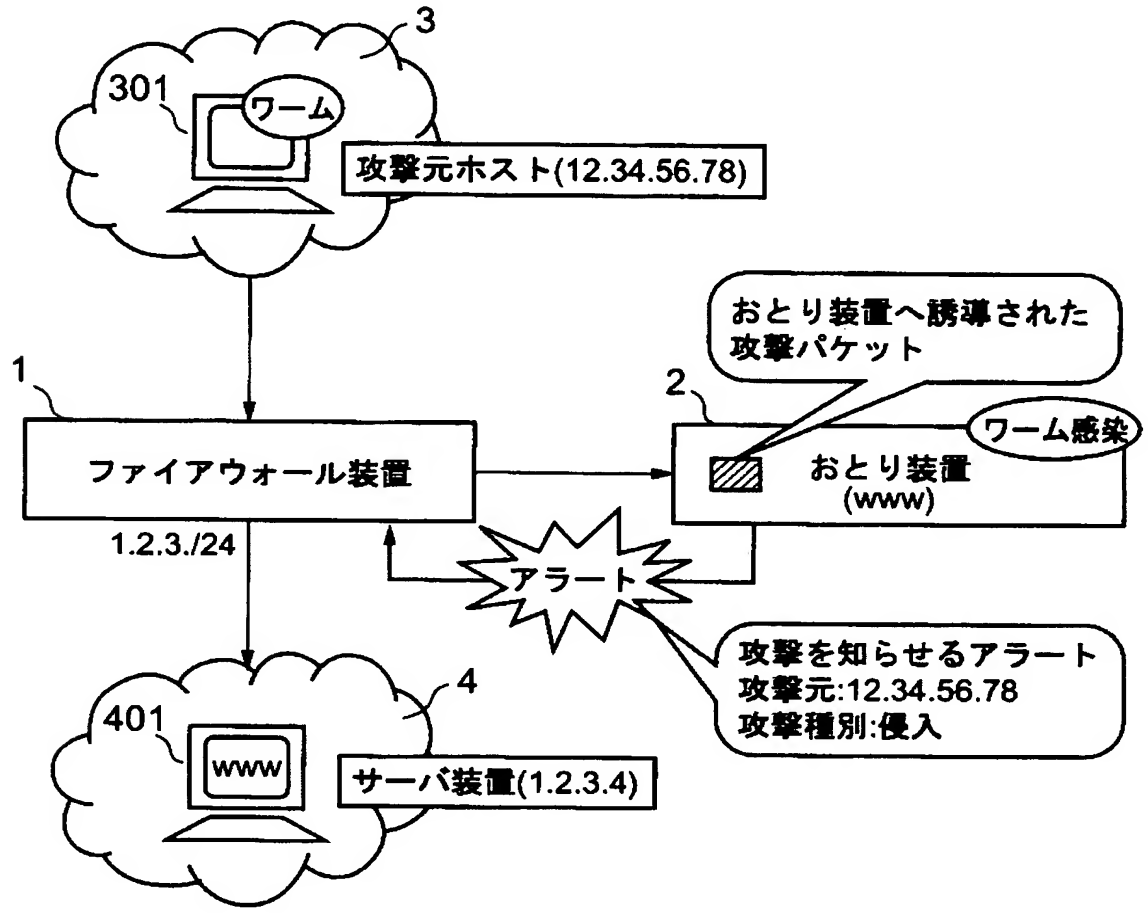
【図９】


3
301
ワーム
攻撃元ホスト(12.34.56.78)
攻撃データを含むパケット
(ソース:12.34.56.78/ディスティネーション:1.2.3.1)
1
ファイアウォール装置
2
おとり装置
(www)
1.2.3./24
4
401
www
サーバ装置(1.2.3.4)

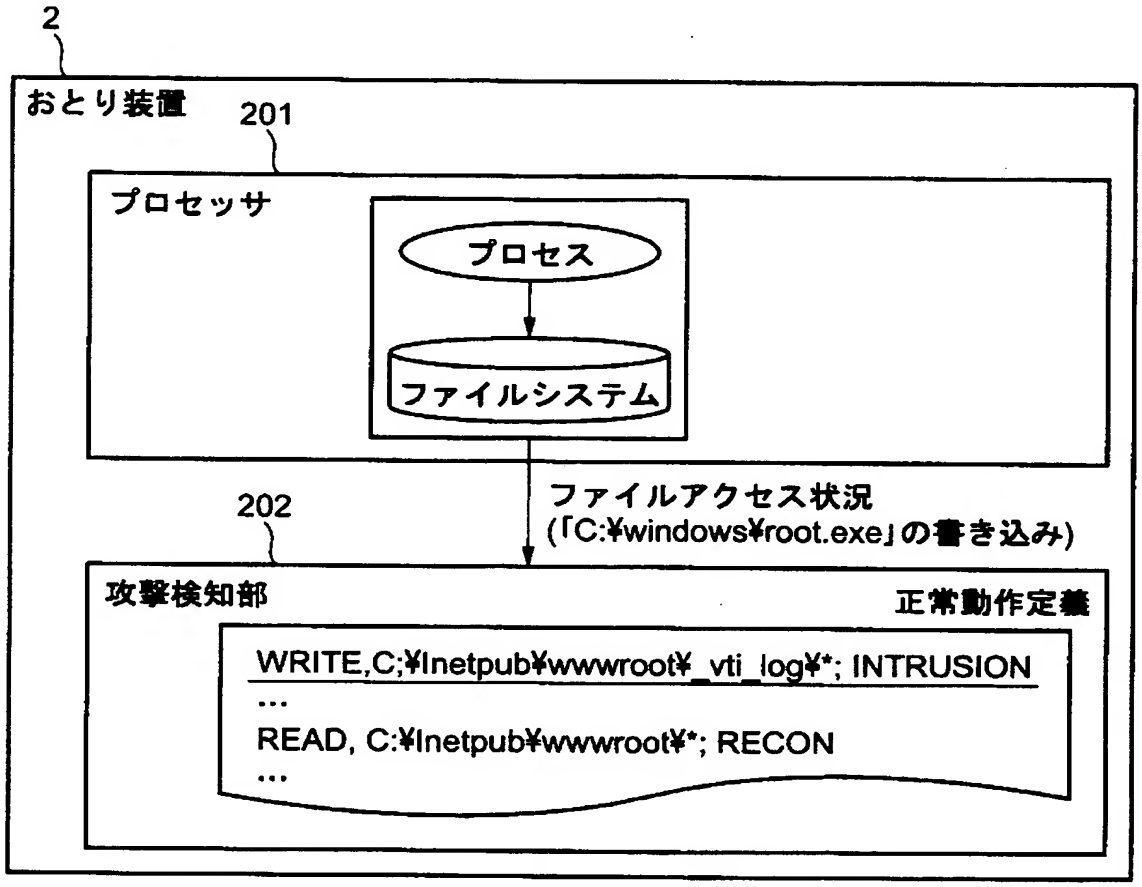
【図１０】


3
301
ワーム
攻撃元ホスト(12.34.56.78)
誘導リストにしたがって、
おとり装置へ誘導された
攻撃パケット
1
2
ファイアウォール装置
おとり装置
(www)
1.2.3./24
1. 2. 3. 1
1. 2. 3. 2
…
誘導リスト
4
401
www
サーバ装置(1.2.3.4)

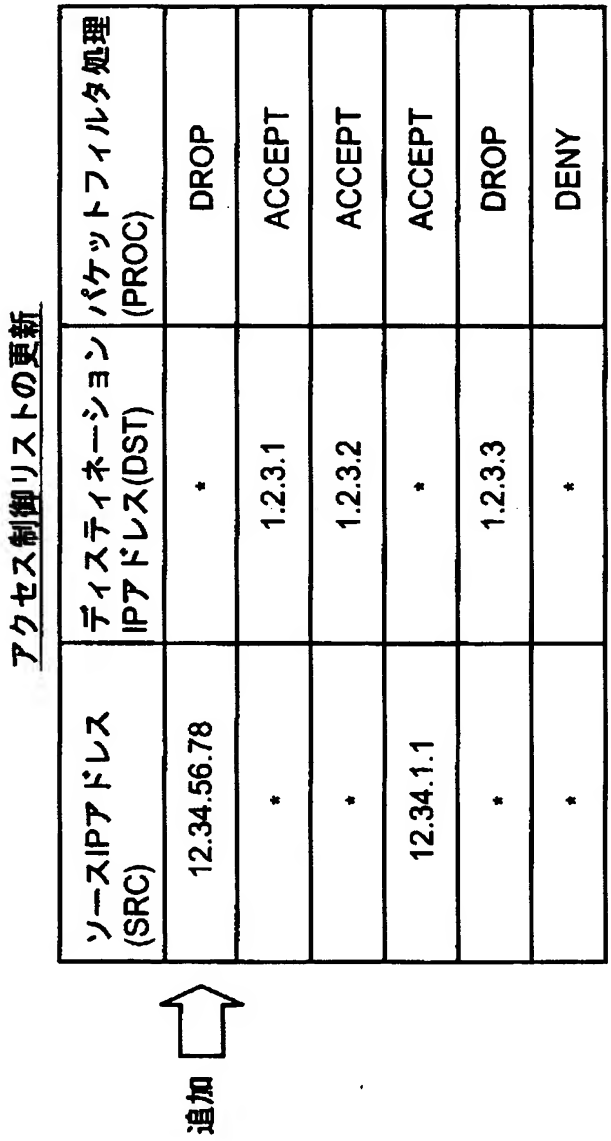
【図１１】


3
301
ワーム
攻撃元ホスト(12.34.56.78)
おとり装置へ誘導された
攻撃パケット
1
2
ワーム感染
ファイアウォール装置
おとり装置
(www)
1.2.3./24
アラート
攻撃を知らせるアラート
攻撃元:12.34.56.78
攻撃種別:侵入
4
401
www
サーバ装置(1.2.3.4)

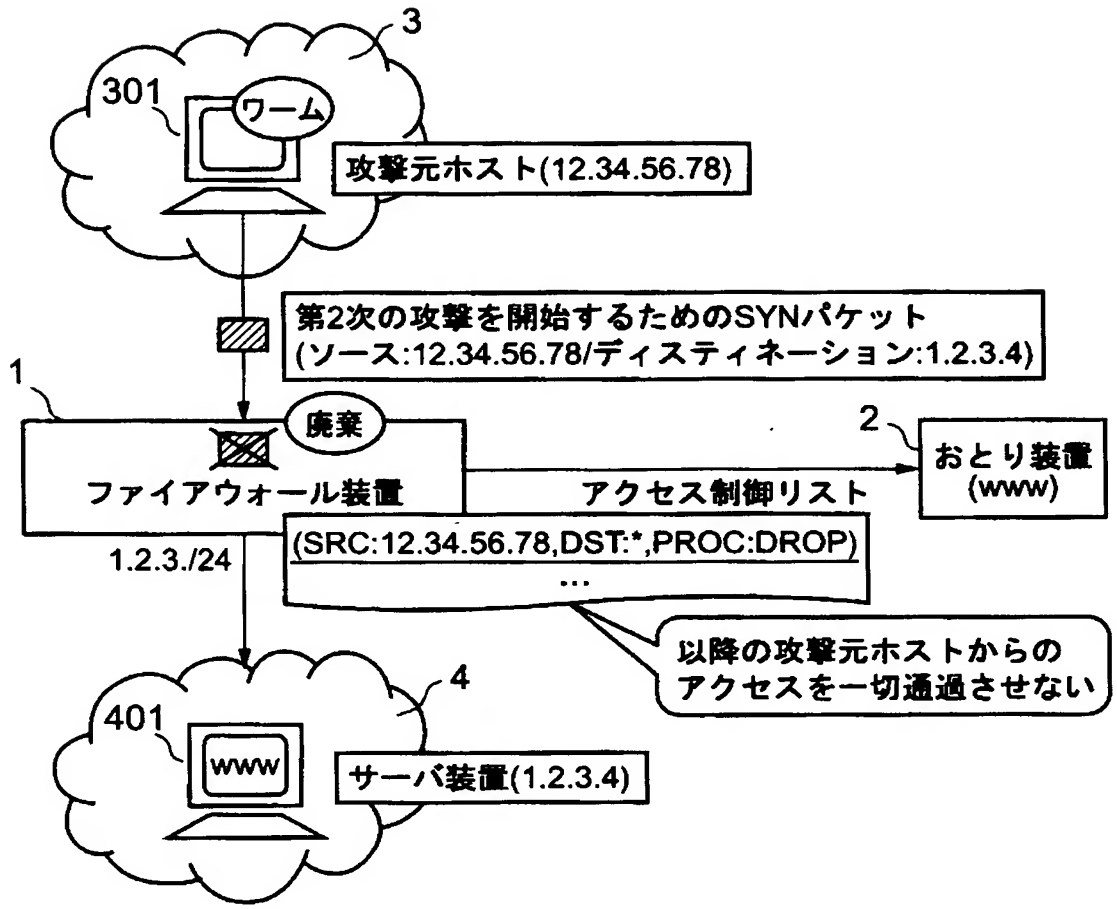
【図１２】


2
おとり装置
201
プロセッサ
プロセス
ファイルシステム
ファイルアクセス状況
(「C:¥windows¥root.exe」の書き込み)
202
攻撃検知部
正常動作定義
WRITE,C;¥Inetpub¥wwwroot¥_vti_log¥*; INTRUSION
...
READ, C:¥Inetpub¥wwwroot¥*; RECON
...

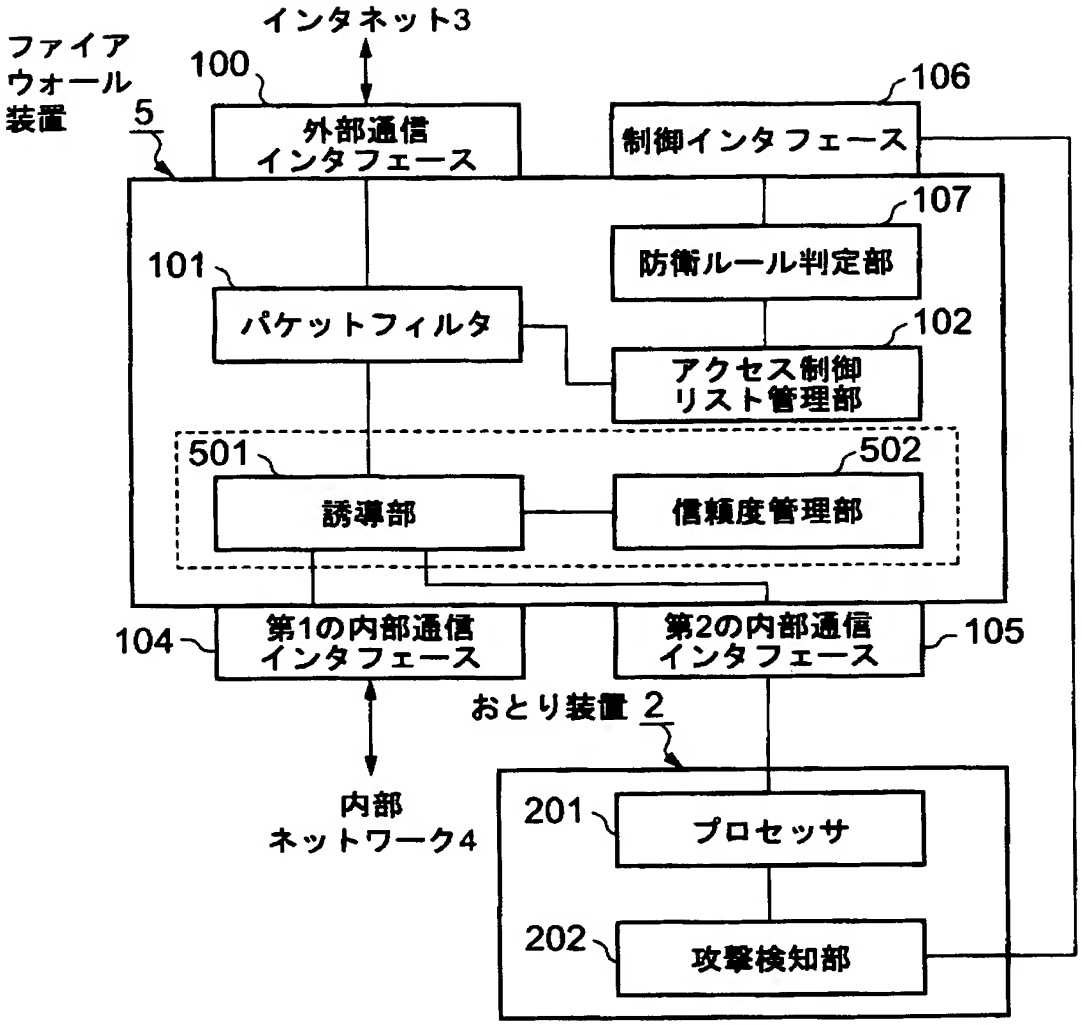
【図１３】


アクセス制御リストの更新
ソースIPアドレス (SRC)
ディスティネーション IPアドレス(DST)
パケットフィルタ処理 (PROC)
12.34.56.78
*
DROP
*
1.2.3.1
ACCEPT
*
1.2.3.2
ACCEPT
12.34.1.1
*
ACCEPT
*
1.2.3.3
DROP
*
*
DENY
追加

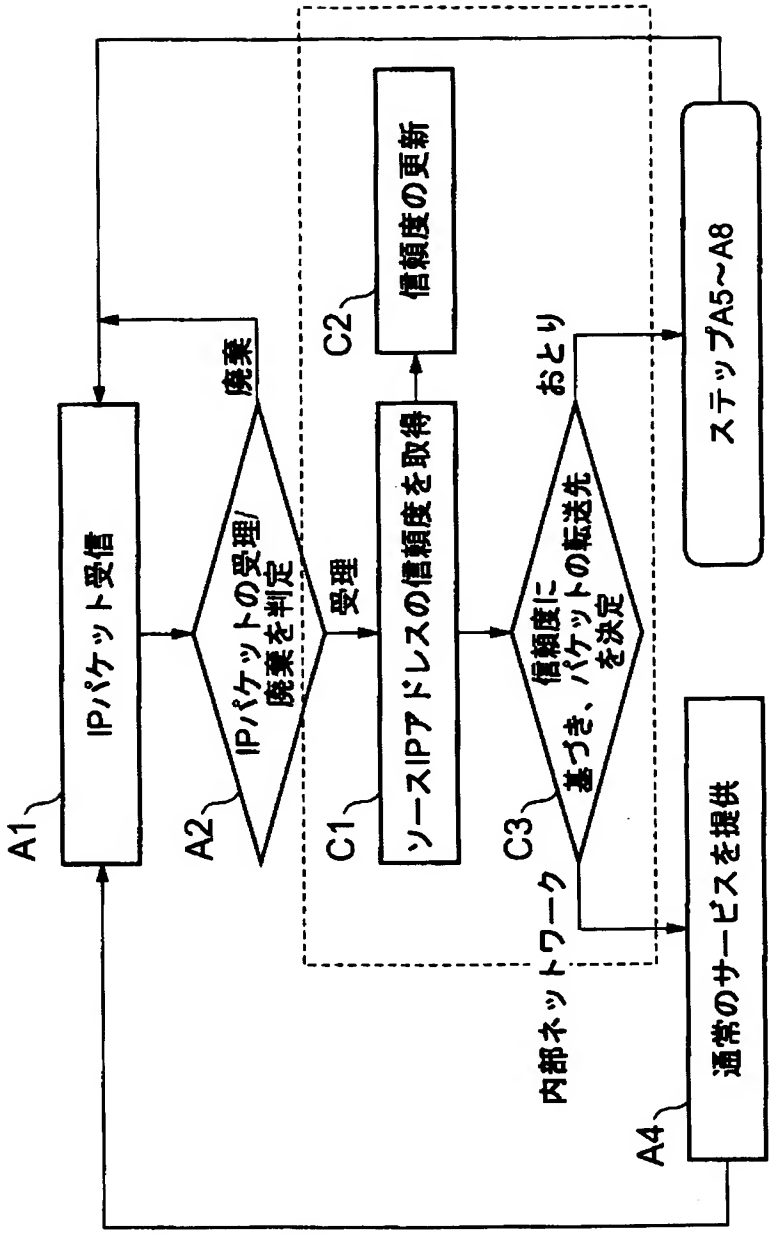
【図１４】


3
301
ワーム
攻撃元ホスト(12.34.56.78)
第2次の攻撃を開始するためのSYNパケット
(ソース:12.34.56.78/ディスティネーション:1.2.3.4)
1
廃棄
ファイアウォール装置
2
おとり装置
(www)
アクセス制御リスト
(SRC:12.34.56.78,DST:*,PROC:DROP)
...
1.2.3./24
以降の攻撃元ホストからの
アクセスを一切通過させない
4
401
www
サーバ装置(1.2.3.4)

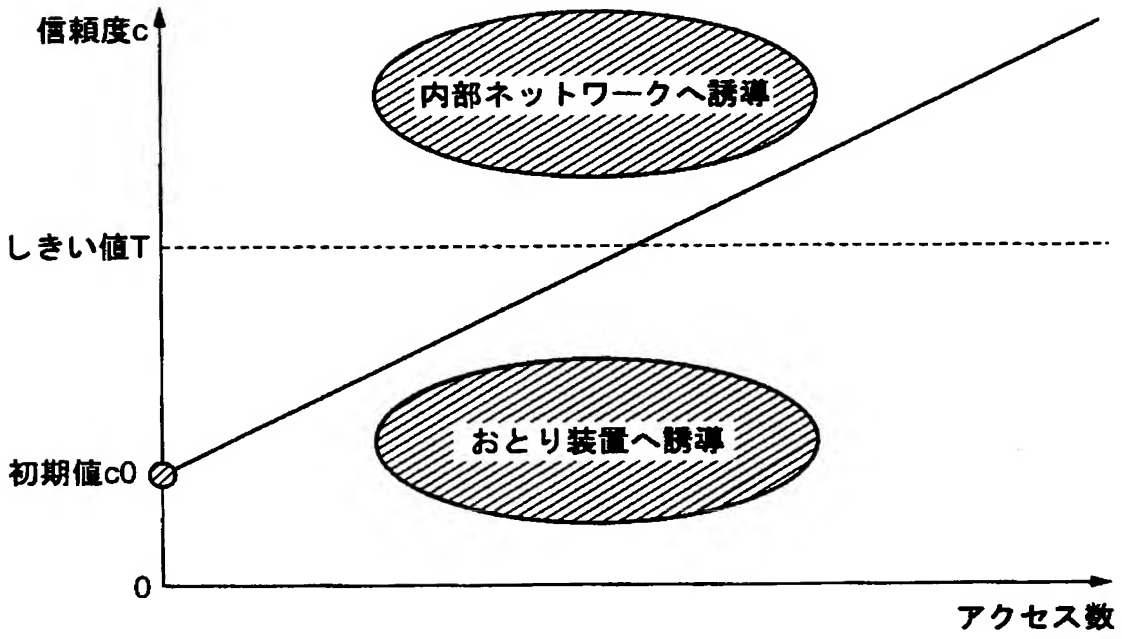
【図１５】


インタネット3
ファイア
ウォール
装置
5
100
外部通信
インタフェース
106
制御インタフェース
107
防衛ルール判定部
101
パケットフィルタ
102
アクセス制御
リスト管理部
501
誘導部
502
信頼度管理部
104
第1の内部通信
インタフェース
第2の内部通信
インタフェース
105
おとり装置 2
内部
ネットワーク4
201
プロセッサ
202
攻撃検知部

【図１６】

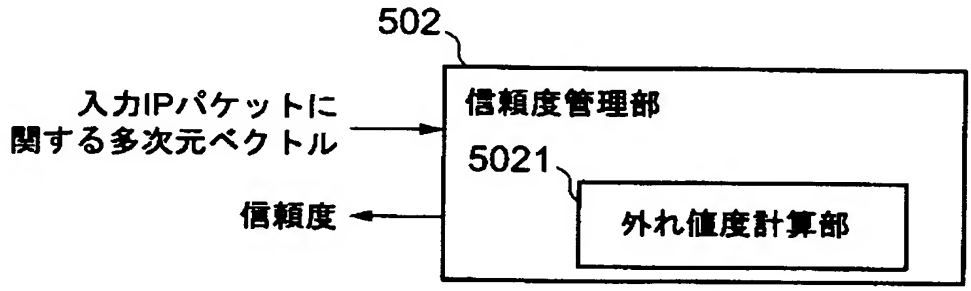

IPパケット受信
A1
IPパケットの受理/
廃棄を判定
A2
廃棄
受理
ソースIPアドレスの信頼度を取得
C1
信頼度の更新
C2
信頼度に
基づき、パケットの転送先
を決定
C3
おとり
ステップA5～A8
内部ネットワーク
通常のサービスを提供
A4

【図１７】

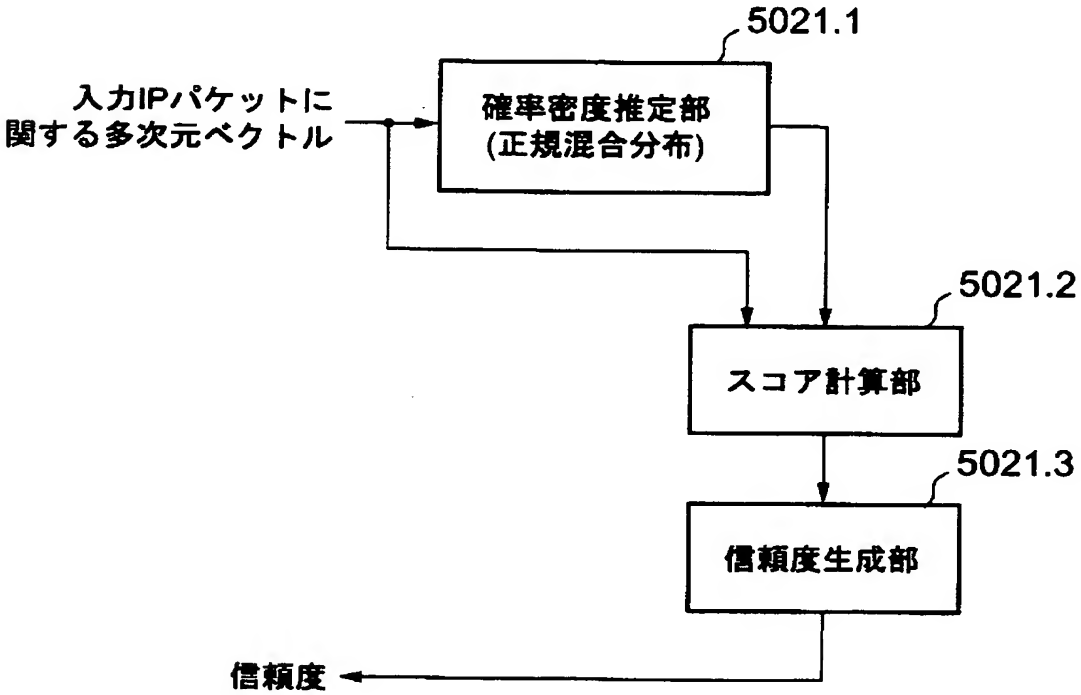


【図１８】

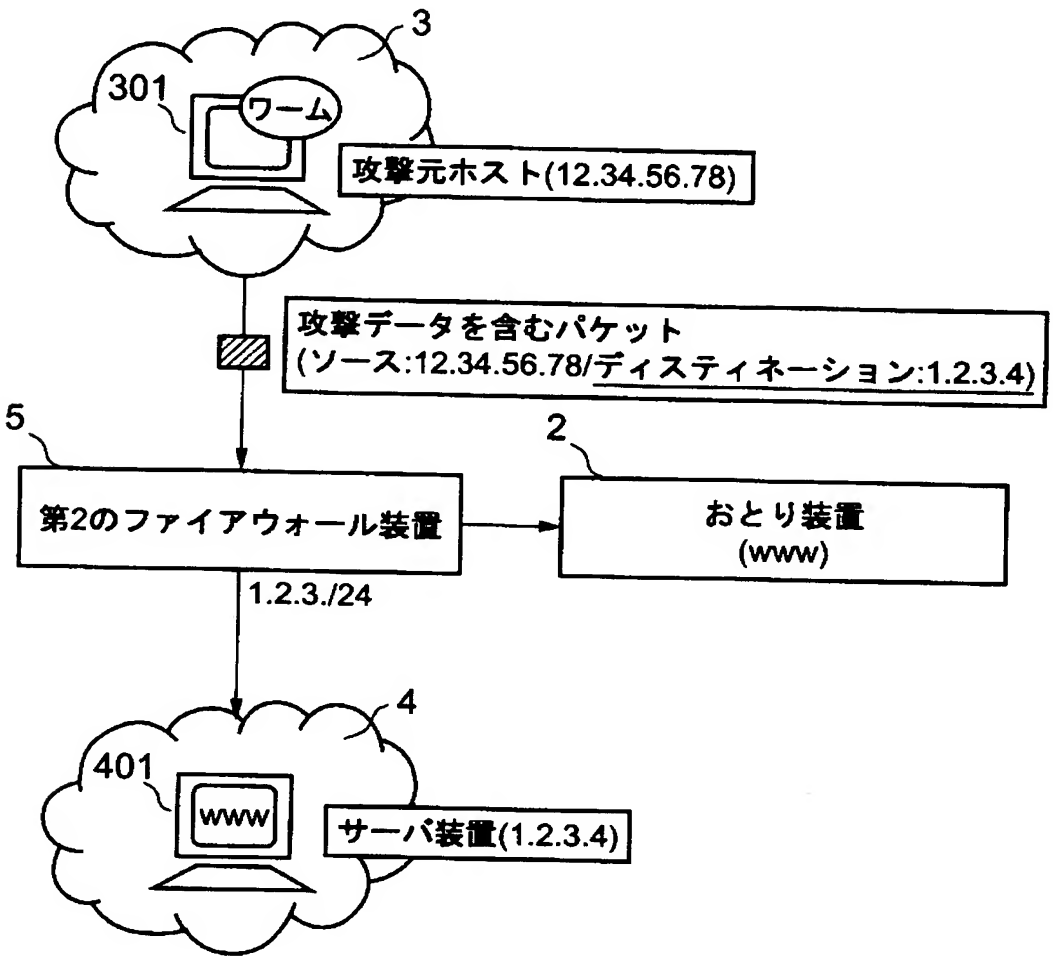
(A)


502
入力IPパケットに
関する多次元ベクトル
信頼度管理部
5021
外れ値度計算部
信頼度

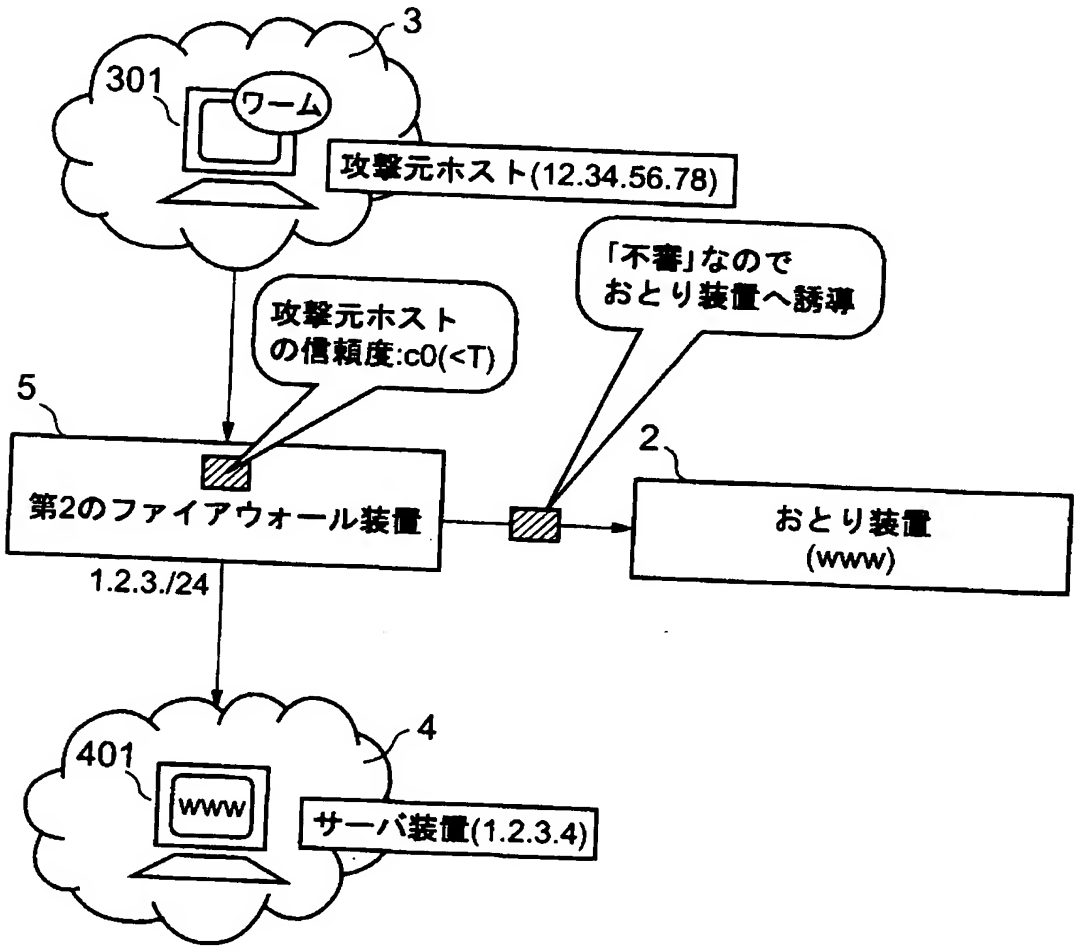
(B)


5021.1
入力IPパケットに
関する多次元ベクトル
確率密度推定部
(正規混合分布)
5021.2
スコア計算部
5021.3
信頼度生成部
信頼度

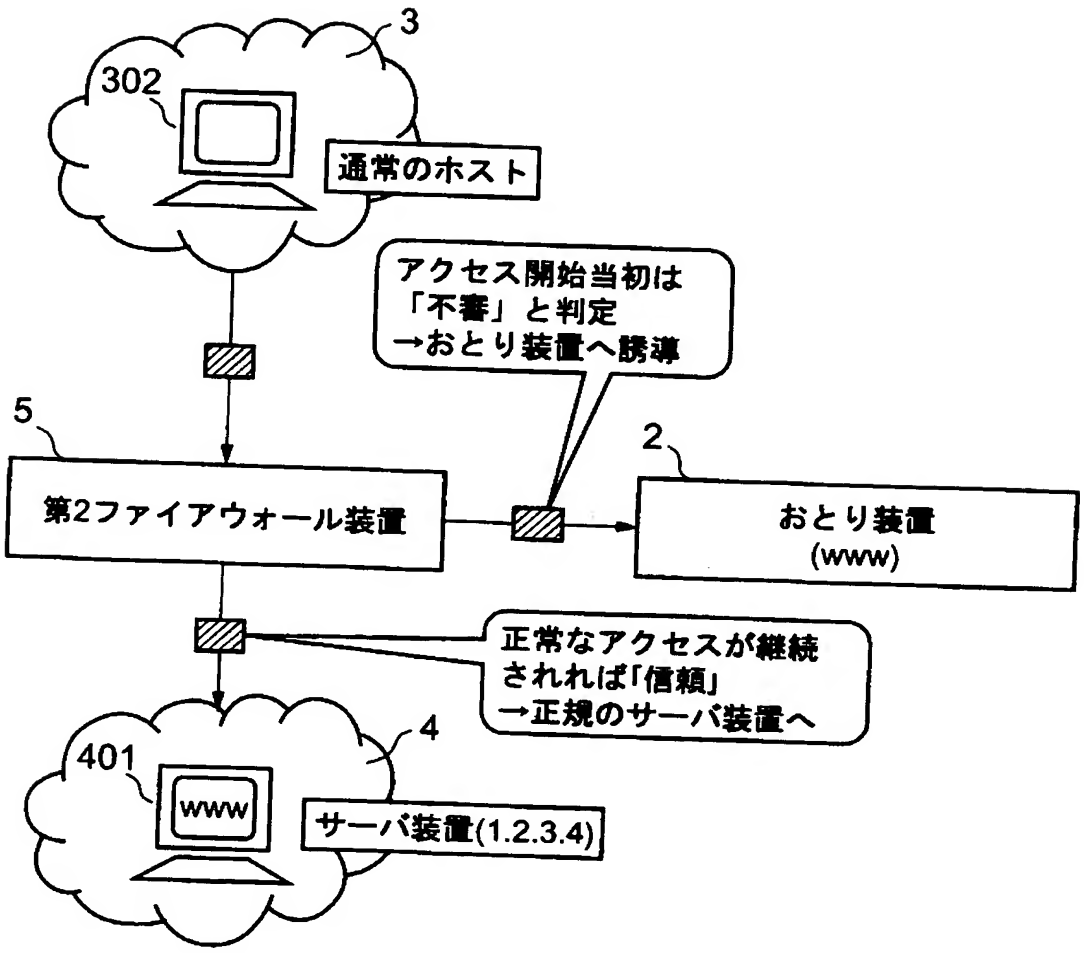
【図１９】


3
301
ワーム
攻撃元ホスト(12.34.56.78)
攻撃データを含むパケット
(ソース:12.34.56.78/ディスティネーション:1.2.3.4)
5
2
第2のファイアウォール装置
おとり装置
(www)
1.2.3./24
4
401
www
サーバ装置(1.2.3.4)

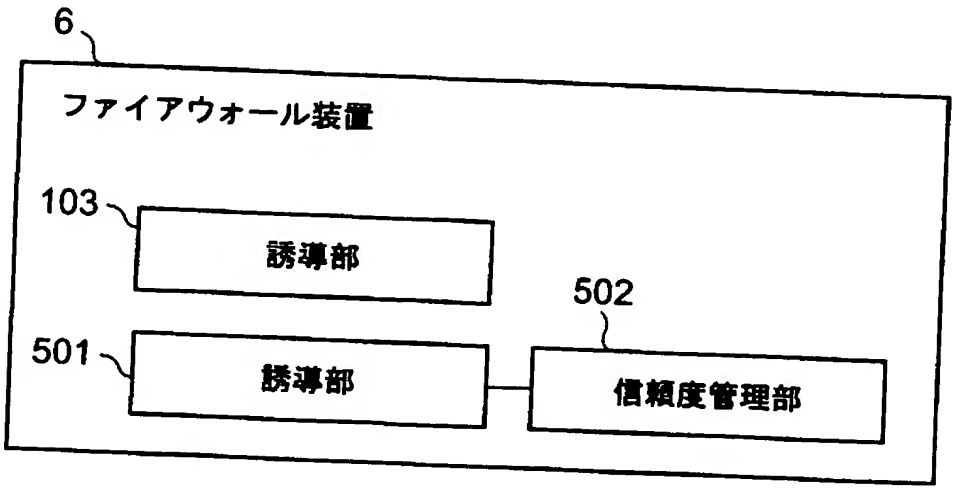
【図２０】


3
301
ワーム
攻撃元ホスト(12.34.56.78)
「不審」なので
おとり装置へ誘導
攻撃元ホスト
の信頼度:c0(<T)
5
2
第2のファイアウォール装置
おとり装置
(www)
1.2.3./24
4
401
www
サーバ装置(1.2.3.4)

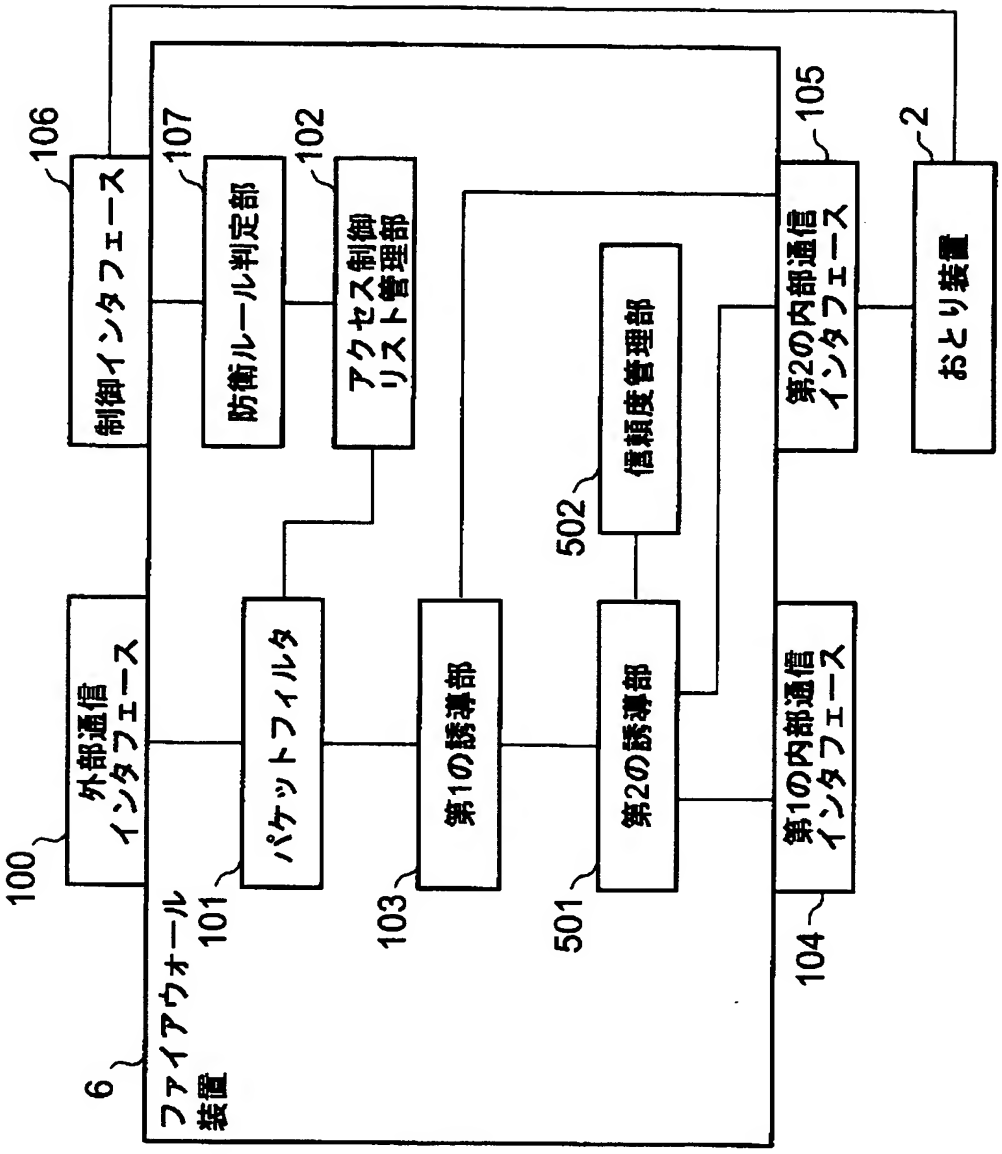
【図２１】


3
302
通常のホスト
アクセス開始当初は
「不審」と判定
→おとり装置へ誘導
5
2
第2ファイアウォール装置
おとり装置
(www)
正常なアクセスが継続
されれば「信頼」
→正規のサーバ装置へ
4
401
www
サーバ装置(1.2.3.4)

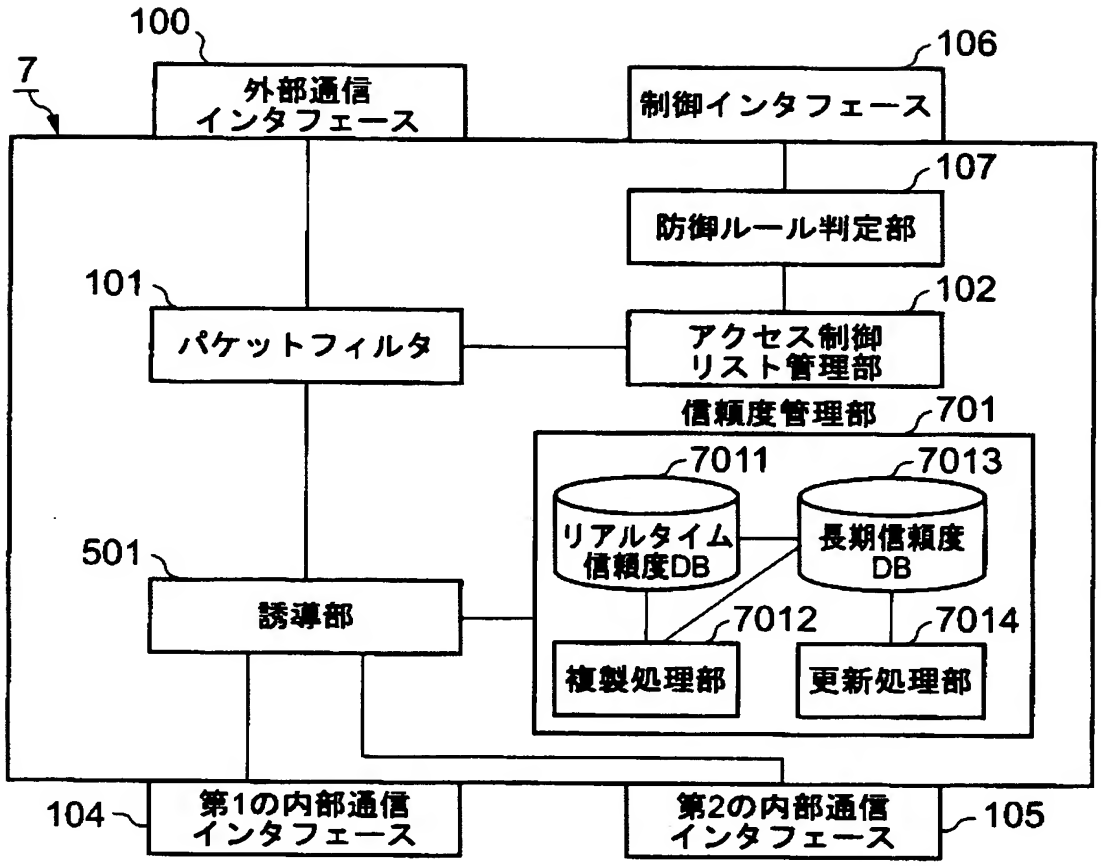
【図２２】



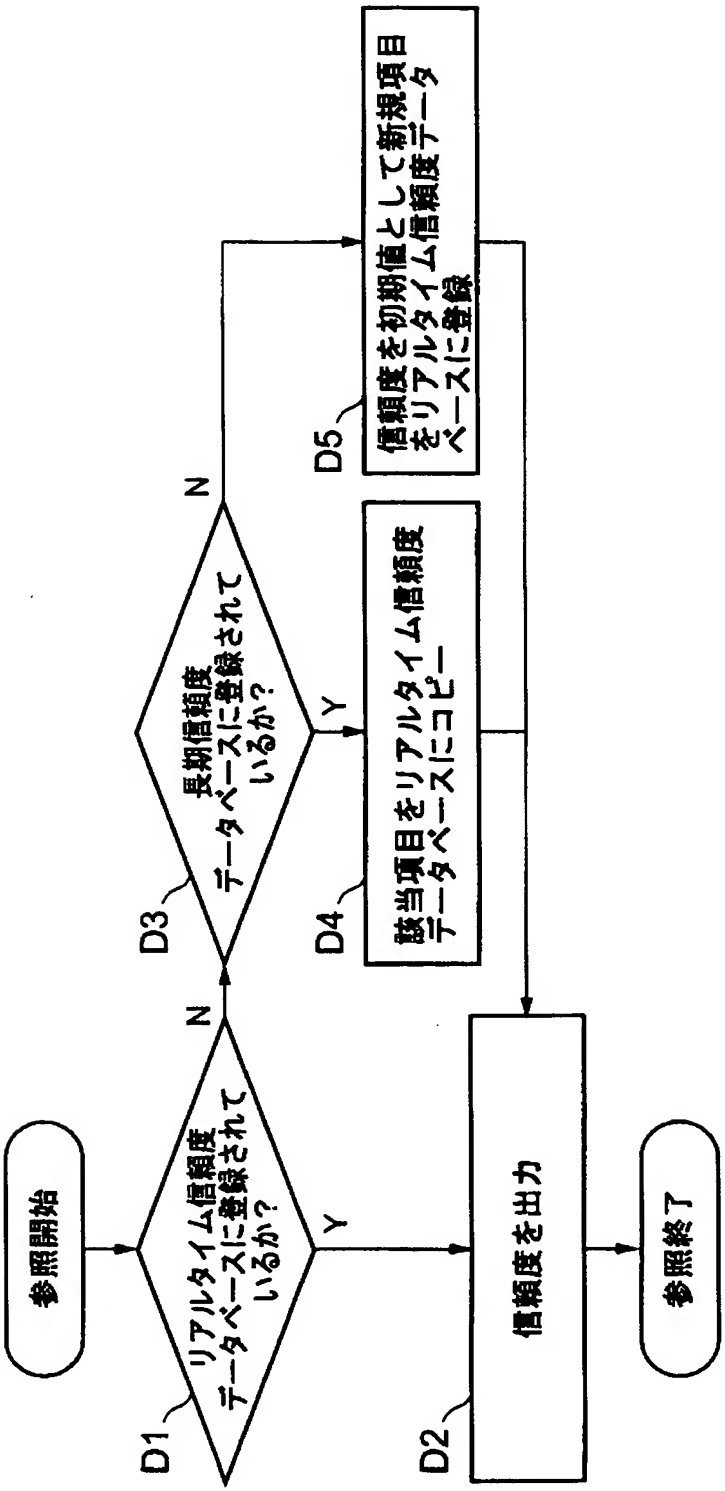
【図２３】


106
107
102
105
2
制御インタフェース
防衛ルール判定部
アクセス制御
リスト管理部
第2の内部通信
インタフェース
おとり装置
502
信頼度管理部
100
外部通信
インタフェース
パケットフィルタ
第1の誘導部
第2の誘導部
第1の内部通信
インタフェース
101
103
501
104
6
ファイアウォール
装置

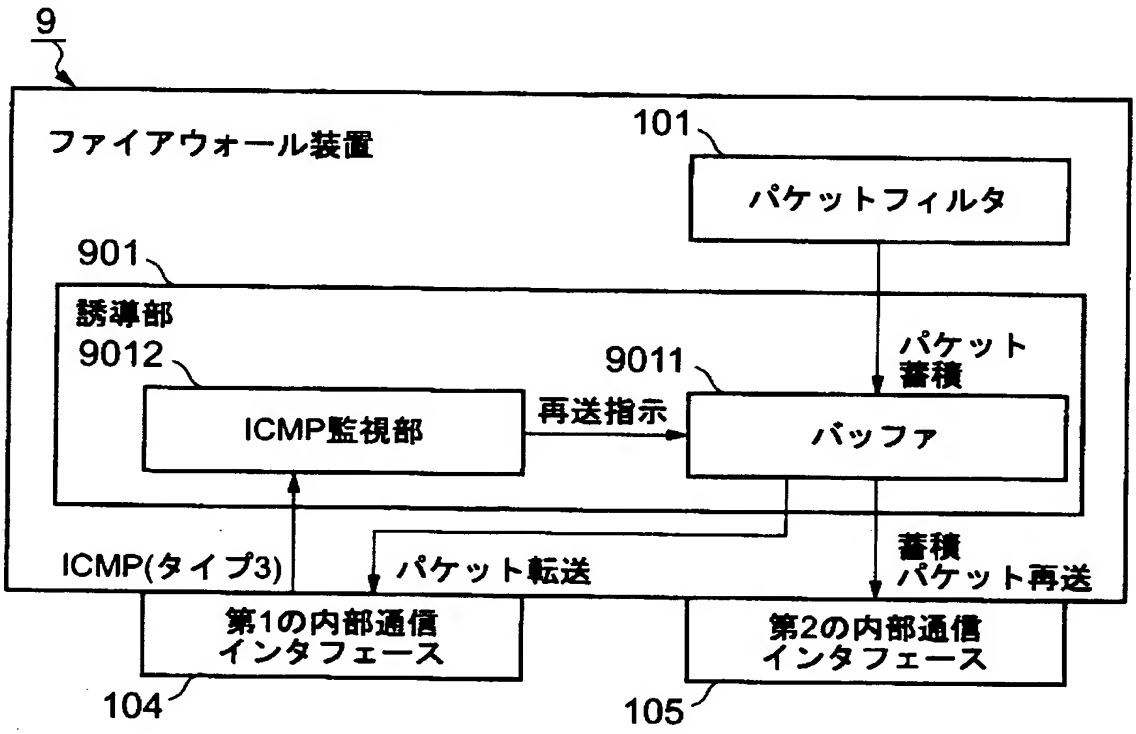
【図２４】


100
7
外部通信
インタフェース
106
制御インタフェース
107
防御ルール判定部
101
パケットフィルタ
102
アクセス制御
リスト管理部
信頼度管理部
701
7011
7013
リアルタイム
信頼度DB
長期信頼度
DB
501
誘導部
7012
7014
複製処理部
更新処理部
104
第1の内部通信
インタフェース
第2の内部通信
インタフェース
105

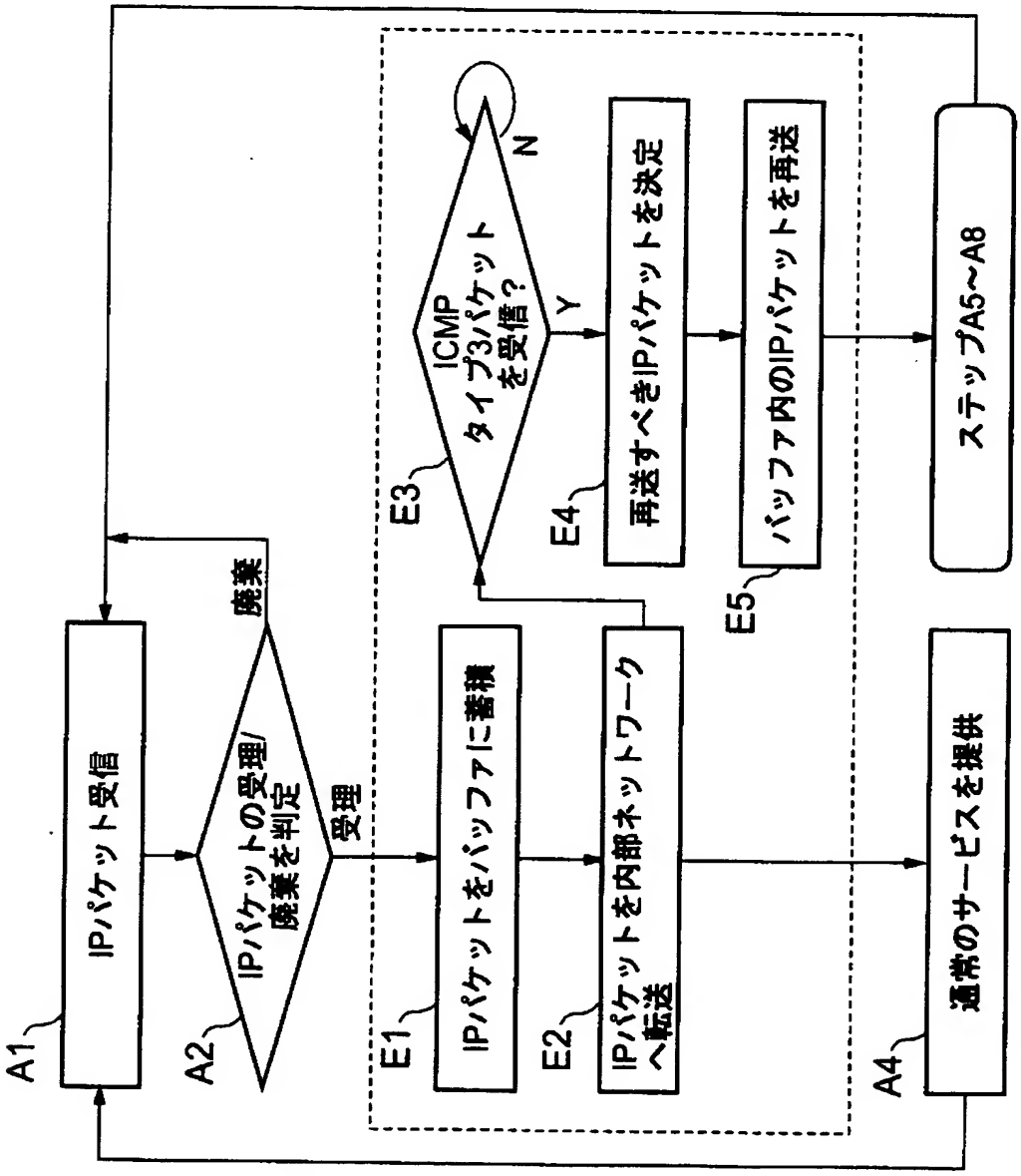
【図２５】


参照開始
リアルタイム信頼度データベースに登録されているか？
D1
N
Y
長期信頼度データベースに登録されているか？
D3
N
Y
該当項目をリアルタイム信頼度データベースにコピー
D4
信頼度を初期値として新規項目をリアルタイム信頼度データベースに登録
D5
信頼度を出力
D2
参照終了

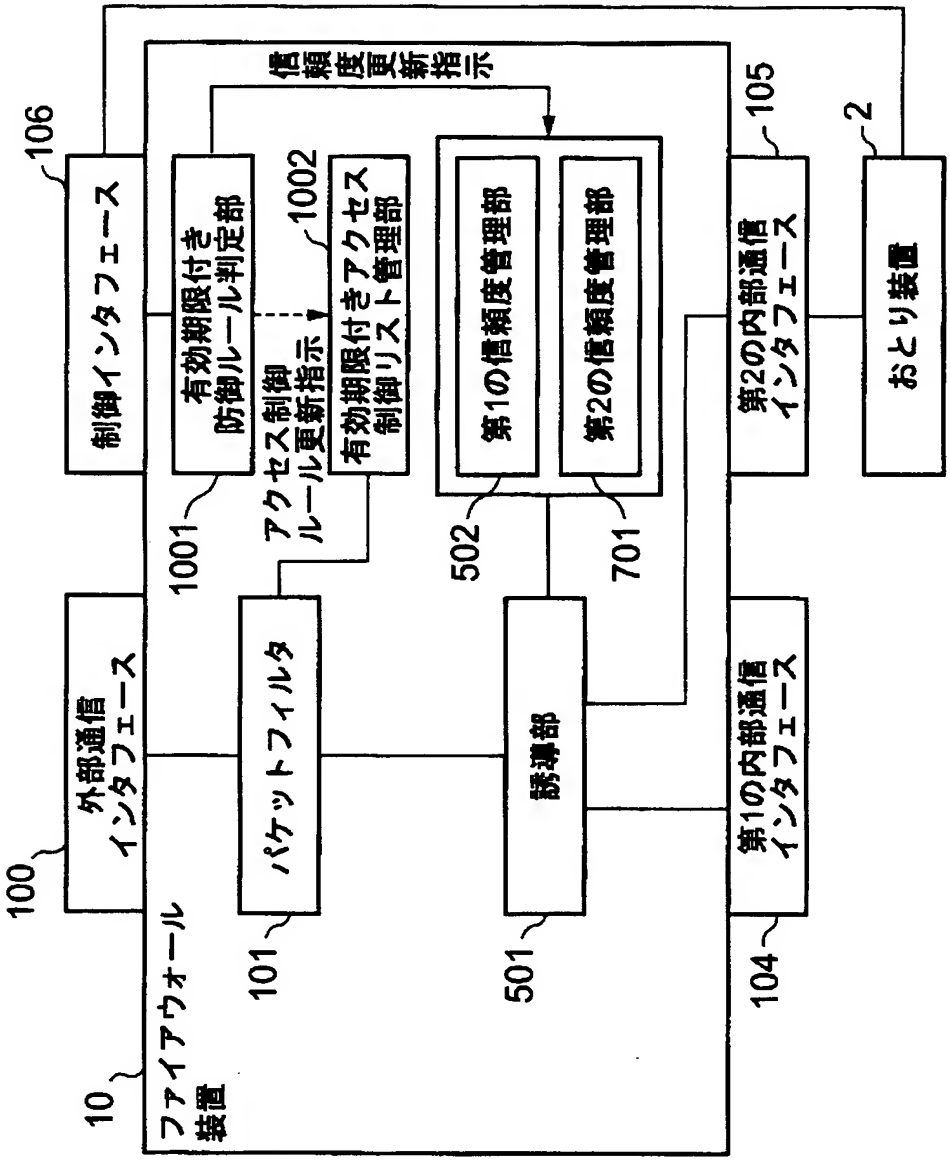
【図２６】


9
ファイアウォール装置
101
パケットフィルタ
901
誘導部
9012
ICMP監視部
9011
パケット
蓄積
再送指示
バッファ
ICMP(タイプ3)
パケット転送
蓄積
パケット再送
第1の内部通信
インタフェース
第2の内部通信
インタフェース
104
105

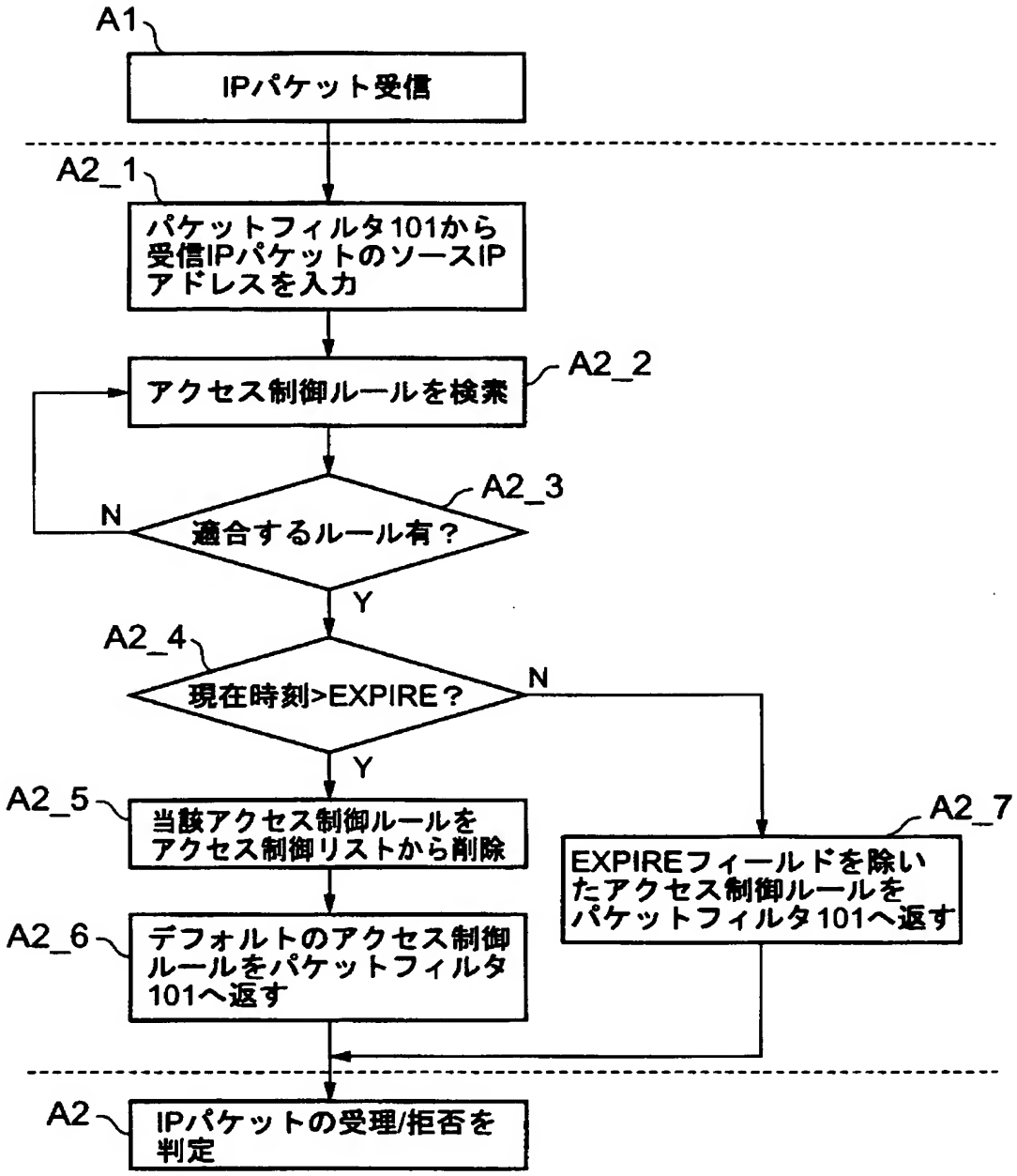
【図２７】


IPパケット受信
A1
IPパケットの受理/
廃棄を判定
A2
廃棄
受理
IPパケットをバッファに蓄積
E1
IPパケットを内部ネットワーク
へ転送
E2
ICMP
タイプ3パケット
を受信?
E3
N
Y
再送すべきIPパケットを決定
E4
バッファ内のIPパケットを再送
E5
ステップA5～A8
通常のサービスを提供
A4

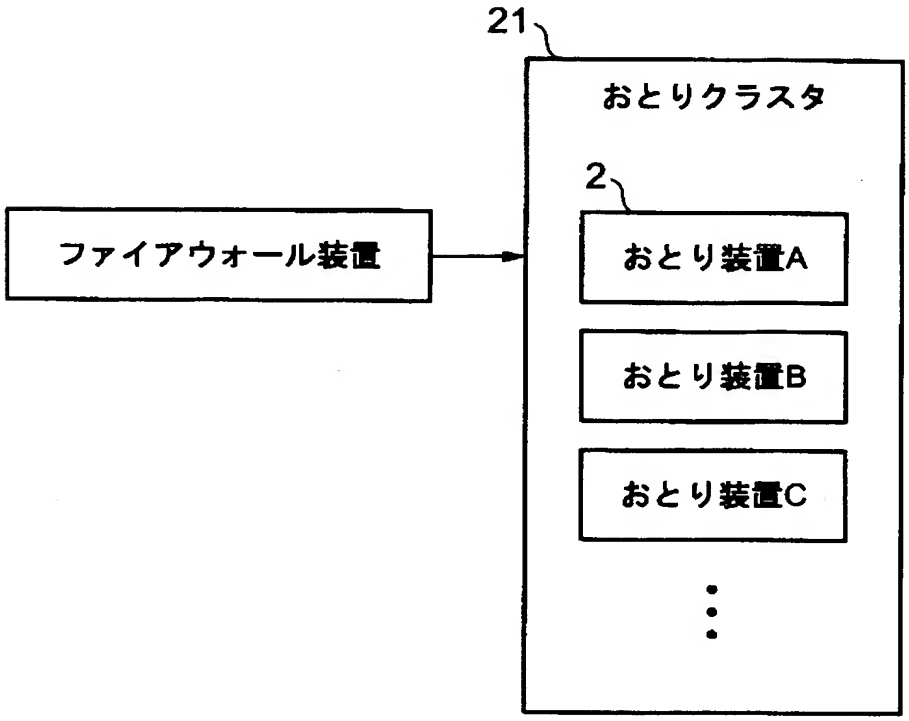
【図２８】


信頼度更新指示
106
制御インタフェース
有効期限付き
防御ルール判定部
1002
有効期限付きアクセス
制御リスト管理部
第1の信頼度管理部
第2の信頼度管理部
105
第2の内部通信
インタフェース
2
おとり装置
アクセス制御
ルール更新指示
1001
502
701
外部通信
インタフェース
パケットフィルタ
誘導部
第1の内部通信
インタフェース
100
101
501
104
ファイアウォール
装置
10

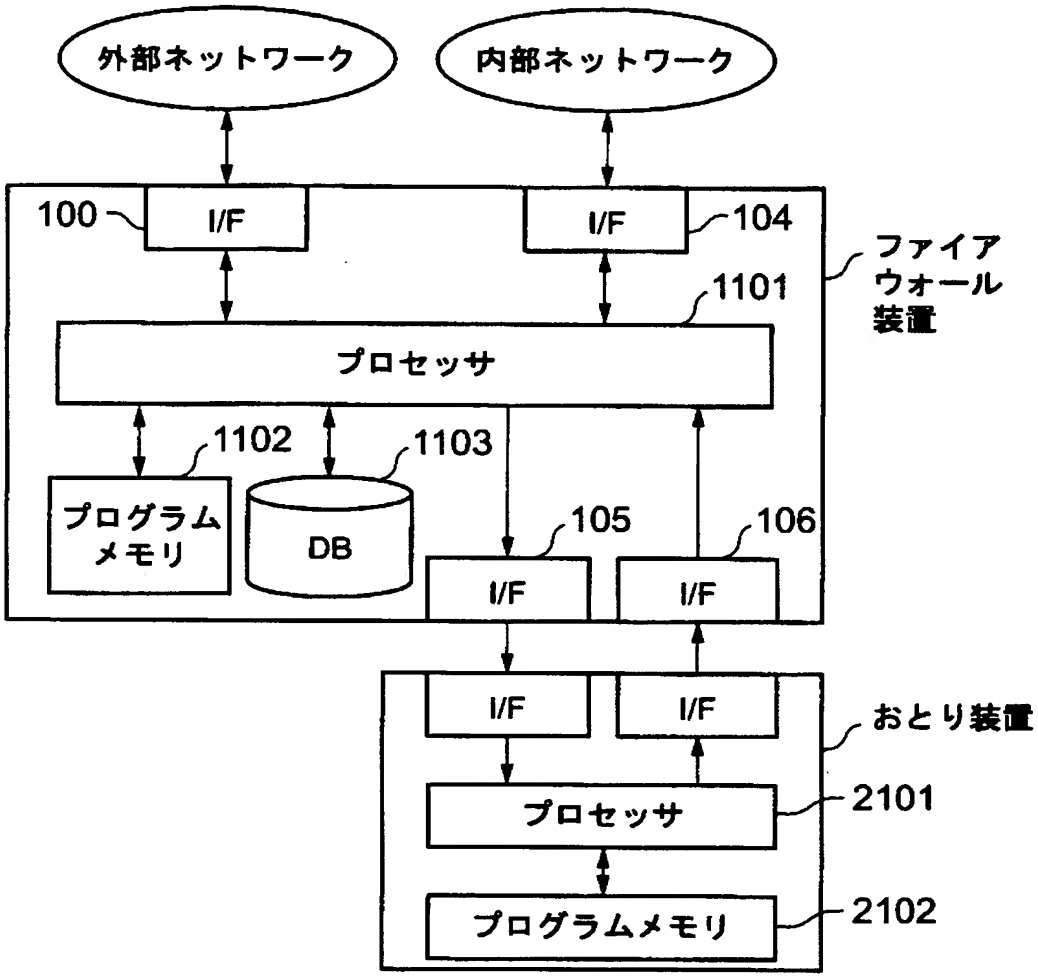
【図２９】


A1
IPパケット受信
A2_1
パケットフィルタ101から受信IPパケットのソースIPアドレスを入力
A2_2
アクセス制御ルールを検索
A2_3
適合するルール有？
N
Y
A2_4
現在時刻>EXPIRE？
N
Y
A2_5
当該アクセス制御ルールをアクセス制御リストから削除
A2_6
デフォルトのアクセス制御ルールをパケットフィルタ101へ返す
A2_7
EXPIREフィールドを除いたアクセス制御ルールをパケットフィルタ101へ返す
A2
IPパケットの受理/拒否を判定

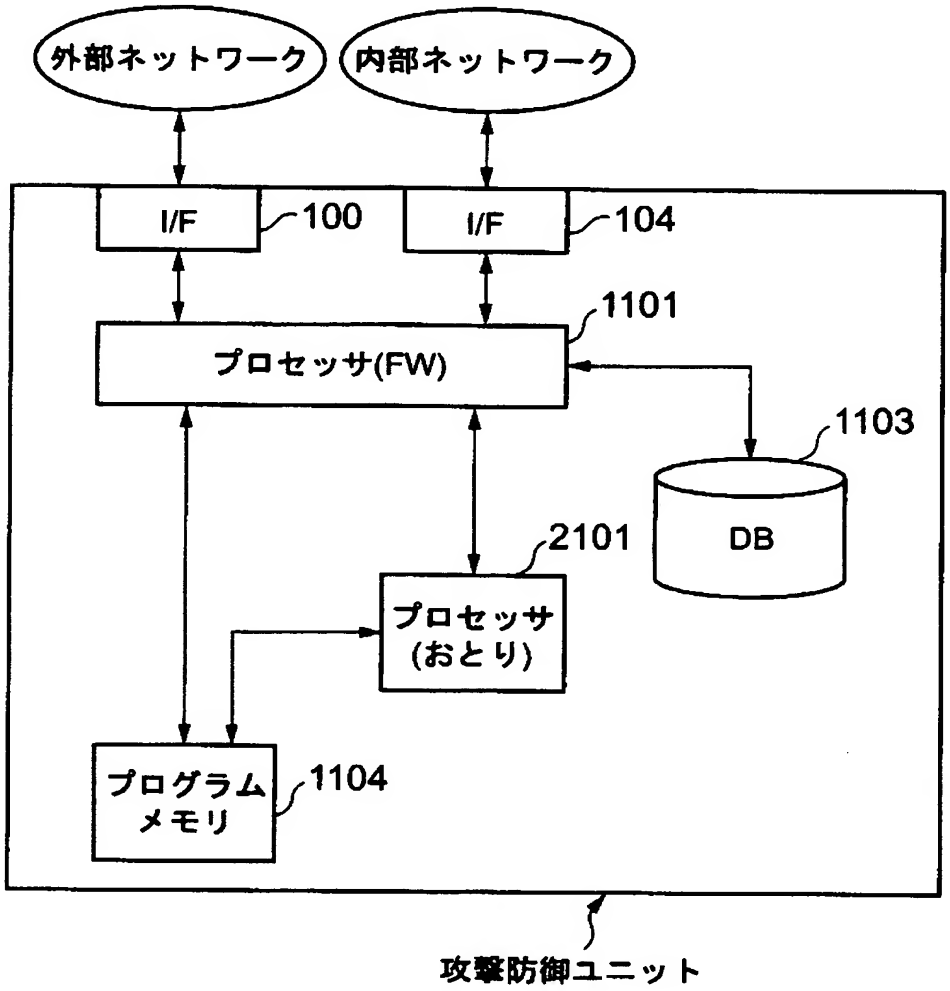
【図３０】



【図３１】


外部ネットワーク
内部ネットワーク
100
I/F
I/F
104
ファイア
ウォール
装置
1101
プロセッサ
1102
1103
プログラム
メモリ
DB
105
106
I/F
I/F
I/F
I/F
おとり装置
2101
プロセッサ
2102
プログラムメモリ

【図３２】


外部ネットワーク
内部ネットワーク
I/F
100
I/F
104
1101
プロセッサ(FW)
1103
DB
2101
プロセッサ
(おとり)
プログラム
メモリ
1104
攻撃防御ユニット

【書類名】　　要約書

【要約】

【課題】　インターネットから内部ネットワークへのアクセスでＳＳＬなど通信路暗号化技術が用いられた場合であっても不正なアクセスを検知し有効に防御する攻撃防御システム及び方法を提供する。

【解決部】　ファイアウォール装置１およびおとり装置２を備え、ファイアウォール装置１では、受け取ったＩＰパケットのヘッダ情報を参照し、所定のルールに基づいて攻撃の可能性がある「不審パケット」をおとり装置２へと誘導する。おとり装置２は、サービスを提供するプロセスを監視しながら、攻撃の有無を判定する。攻撃を検出した際には、攻撃元ホストのＩＰアドレスを含むアラートを生成してファイアウォール装置１に伝達する。当該アラートを受けたファイアウォール装置１は、以降、攻撃元ホストからのＩＰパケットの受入れを拒否する。

【選択図】　　図２

特願２００２－２３８９８９

出　願　人　履　歴　情　報

識別番号　　［０００００４２３７］

１．変更年月日　　１９９０年　８月２９日
［変更理由］　　新規登録
住　所　　東京都港区芝五丁目７番１号
氏　名　　日本電気株式会社